# SECURITY SPECIFICATION LANGUAGE FOR DISTRIBUTED HEALTH INFORMATION SYSTEM (DHIS)

INTAN NAJUA BINTI KAMAL NASIR

DEPARTMENT OF COMPUTER AND INFORMATION SCIENCES
UNIVERSITI TEKNOLOGI PETRONAS
JULY 2009

**Status of Thesis**

Title of thesis: Security Specification Language for Distributed Health Information System (DiHIS)

I INTAN NAJUA BINTI KAMAL NASIR hereby allow my thesis to be placed at the Information Resource Center (IRC) of Universiti Teknologi PETRONAS (UTP) with the following conditions:

1. The thesis becomes the property of UTP
2. The IRC of UTP may make copies of the thesis for academic purposes only.
3. This thesis is classified as

☐ Confidential

☑ Non-confidential

The contents of the thesis will remain confidential for _____ years.

Remarks on disclosure:

_____

Endorsed by

Intan Najua binti Kamal Nasir
Department of Computer
Information Sciences (CIS)
Universiti Teknologi PETRONAS
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzuan.
Date: _____

Azween bin Abdullah
Department of Computer and
Information Sciences (CIS)
Universiti Teknologi PETRONAS
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzuan.
Date: 15/7/09.

## Approval Page

UNIVERSITI TEKNOLOGI PETRONAS

Approval by Supervisor (s)

The undersigned certify that they have read, and recommend to The Postgraduate Studies Programme for acceptance, a thesis entitle "**Security Specification Language for Distributed Health Information System (DiHIS)**" submitted by **Intan Najua binti Kamal Nasir** for the fulfillment of the requirements for the degree of Master of Science (MSc) in Information Technology by Research.

Signature : _____

Main Supervisor : Dr Azween Bin Abdullah
Senior Lecturer
Information Technology/Information Systems
Universiti Teknologi PETRONAS
31750 Tronoh
Perak Darul Ridzuan

Date : 15/7/09

Co-Supervisor : _____

**Title Page**

UNIVERSITI TEKNOLOGI PETRONAS

Security Specification Language for Distributed Health Information System (DiHIS)

By

Intan Najua binti Kamal Nasir

A THESIS

SUBMITTED TO THE POSTGRADUATE STUDIES PROGRAMME

AS A REQUIREMENT FOR THE

DEGREE OF MASTER OF SCIENCE (MSc)

IN INFORMATION TECHNOLOGY

BANDAR SERI ISKANDAR,

PERAK,

JULY, 2009

**Declaration**

I hereby declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that is has not been previously or concurrently submitted for any other degree at UTP or other institutions.

Signature : _____

Name : INTAN NAJUA BT KAMAL NASIR

Date : 16/07/09

**Acknowledgement**

First and foremost, I am grateful to Allah for giving me the chance to study, meet and work with great people at this prestigious university, for His kindness, mercy and assistance until I managed to finish this research.

Thousand of appreciations to my family who has given motivational support and trust in me. Their faith has brought me up at the time I was losing mine.

I want to thank in particular to my supervisor, Dr. Azween Abdullah for valuable input, countless effort, assistance and encouragement since the first day I started until the moment I finished my studies. May Allah bless him and his family for his patience and sincerity shown to me in two years.

Not forgetting, lecturers in Computer and Information Science Department, Universiti Teknologi PETRONAS; AP Dr. Ahmad Kamil Mahmood, Dr. Wan Fatimah Wan Ahmad, AP Dr. Abas bin Md Said, Mr. Abdullah Sani Abd Rahman, Dr. Dhanapal Durai Dominic, Mr. Lukman bin Abdul Rahim, and all lecturers for their assistant directly or indirectly in completing my research and for their valuable assistance and encouragement. Not to leave behind, Prof. Farhad Arbab, the visiting professor and Dr. Etienne Scheneider, for their compassion in reviewing the thesis. Only Allah can repay their effort.

Special appreciation to all staffs at the Postgraduate Office especially to Major Borhan bin Ismail and Mrs. Kamaliah Mohd for their friendliness and effective services.

I wish to thank staffs at the Ministry of Health Mrs. Zarimah Jumari, Mrs. Umi Kalsom Adam, and staff at Pusat Perubatan Ar Ridzuan, Mr. Mohd Harizan Hassan, and Mrs. Jenny Yap from Ipoh Specialist Hospital for their hospitality during the interview sessions.

Last but not least, appreciation to dear colleagues who always lend their ears, eyes, time and effort without asking anything in return. In particular to Mr. Yasir Abdelgadir Batira; who has shared the valuable experiences with me through the process of writing this thesis. Thanks a lot to Mr. Syed Nasir Mehmood Shah for his generosity in giving ideas and to all members of research group who always gave never ending motivations.

## Abstract

The introduction of policy based management which to manage distributed, complex and numerous systems is widely accepted and used in various sectors. The policy creators create policies that suit best for their operations and management. Since there are numerous of policies, this research focuses on the security policies only which are appointed to the distributed system of health information system. In order to implement the security policies, we need a language that can represent the security policies for distributed health information system completely. From the literature review conducted, there are numerous of security languages have been introduced since two decades ago. Those languages carry their own approaches representing the security policy and some of them do not support the characteristics of distributed system. There is no security language to implement the security policy for distributed health information system. This thesis introduces and initiates a security language to implement security policies in distributed health information system called DiHIS. Adding to that, there are three existing security languages used for discussion and comparison with the proposed DiHIS security language. They are ASL, LaSCO and Ponder. DiHIS security language has shown that it is able to represent the Security Policy Model for Clinical Information System completely compares to those three security languages. This language also has an added value when it covers the Need To Know Policy which other security languages do not. Need To Know Policy is one of the crucial issues in the health sector. DiHIS security language has also been tested with the application domain in health information system. The strength of the language can be seen with the ability of DiHIS to represent the security policies in various connections between various organizations involved in distributed health information system.

**Abstrak**

Pengurusan berasaskan polisi telah diperkenalkan demi memudahkan mengawal selia sejumlah besar sistem-sistem yang terlibat dalam rangkaian termasuklah sistem yang kompleks. Penerimaan pegurusan berasakan polisi amat disenangi dan diterima ramai dari semua sektor. Penggubal polisi akan menggubal polisi yang bersesuaian dengan operasi dan pengurusan masing-masing. Terdapat berbagai jenis polisi yang berbeza-beza yang telah dikuat kuasakan. Namun, kajian ini memberikan tumpuan kepada polisi keselamatan di mana ianya menjurus kepada rangkaian sistem maklumat kesihatan sahaja. Untuk merealisasikan polisi-polisi ini, kita memerlukan bahasa keselamatan yang boleh menguatkuasakan polisi tersebut khusus untuk rangkaian sistem maklumat kesihatan. Berdasarkan daripada kajian yang telah dijalankan, terdapat banyak bahasa keselamatan yang telah dicipta sejak dua puluh tahun yang lalu. Setiap bahasa itu mempunyai cara yang tersendiri untuk menguatkuasakan polisi keselamatan malahan terdapat juga beberapa bahasa yang tidak dapat menampung keadaan rangkaian sistem yang sangat kompleks. Tambahan lagi, bahasa-bahasa yang telah tersedia itu tidak satupun dapat menyokong keadaan rangkaian sistem maklumat keselamatan dengan sepenuhnya. Tesis ini memperkenalkan satu bahasa keselamatan yang baru khusus untuk menguatkuasakan polisi keselamatan di dalam rangkaian sistem keselamatan kesihatan yang dinamakan DiHIS. Tiga bahasa keselamatan telah dipilih daripada bahasa-bahasa keselamatan yang tersedia. Bahasa-bahasa ini digunakan untuk membuat perbandingan dengan DiHIS. Tiga bahasa tesebut adalah ASL, LaSCO dan Ponder. Hasil kajian menunjukkan DIHIS berjaya menguatkuasakan suatu model polisi keselamatan khusus untuk sistem maklumat klinikal sepenuhnya apabila dibandingkan dengan tiga bahasa tersebut. Di samping itu, DiHIS juga mempunyai kelebihan di mana ia menguatkuasakan polisi perlu tahu yang mana tidak dikuatkuasakan oleh bahasa yang lain. Polisi perlu tahu adalah salah satu isu yang sangat penting di dalam rangkaian sistem maklumat kesihatan. DiHIS juga telah diuji dalam satu kajian rangkaian sistem maklumat kesihatan untuk menguatkuasakan polisi-polisi yang terdapat di dalam rangkaian tersebut. Kelebihan DiHIS terserlah apabila bahasa itu mampu menguatkuasakan polisi-polisi keselamatan yang ditetapkan di antara organisasi yang terlibat di dalam rangkaian sistem maklumat kesihatan.

## Table of Contents

## List of Table

## List of Figures

## List of Symbols and their Meaning

| | |
|---|---|
| Level | L |
| Object | O |
| Subject | S |
| General policies | P |
| Sub-policies | Q |
| Additional policies | D |
| Function | f |
| Transaction | T |
| Target | R |
| Identification | ID |
| Type | Typ |
| Action | a |
| Access granted | $+\sigma$ |
| Access denied | $-\sigma$ |
| Then | $\therefore$ |
| Where | \| |
| Allow to Open | +open |
| Apply | ~ |
| When | $\phi$ |
| Date | D |
| Delete From | ⊠ |
| Computer system | $\alpha$ |
| Time | t |
| The system operation: send | Send (Destination, Data) |
| The system operation: receive | Receive (Source, Data) |
| The system operation: compare | Compare (Built-In, Data) |
| The system operation : verb | Verb ( Original → Value after Modify) |

| | |
|---|---|
| Authorized Entity | E |
| To | ⇨ |
| Lab material | ∝ |
| Lab result | ∞ |
| Month | M |
| Number of members in set x | number[x] |

# CHAPTER ONE

# INTRODUCTION

## 1.1 Background of Research Area

Back in 1948, United Kingdom has introduced its National Health Services (NHS). NHS was funded to provide free of charge comprehensive treatment for the British public (J.Michele 1999). In India, Apollo private hospitals group have commenced Apollo Telemedicine Networking Foundation (ATNF) which has been serving the country for almost three decades. The purpose of ATNF is to connect the Apollo hospitals with other Apollo Hospitals regardless of the location whether it is inside the country or abroad. In 2003, ATNF has jumped into collaboration with Indian Space Research Organization (ISRO) with the purpose to provide healthcare services to rural and distributed in distant geographical locations apart from the high density urban areas (May 2003). In New Zealand, they deployed New Zealand Telepaediatric Service (NZTPS) in order to overcome barriers for doctors to access patients in isolated regions (Ramos 2007). In Pakistan, Health Management Information System (HMIS) was developed in the early 1990s. In United State, they implemented Nationwide Health Information Network (NHIN) which consists of several networks that are connected with each other. NHIN keep revolutionizing following the president's Bush goal for most American to have access to secure electronic health records by 2014. In 2003, the German Federal Ministry

for Healthcare and Social Security launched the bIT4health (better IT for better health) with the purpose of cost savings, improvement of patient's safety as well as basic services, reduce medication errors or wrong information provided (Bernd Blobel 2007). Based on that, health institutions are moving forward with the implementation of Information Technology (IT). In return, they have system called Health Information System (HIS). Realizing the importance and the advantage of HIS, other countries such as Singapore as cited in (J. Lavanya 2006) have been implementing the HIS which derived from the Personal Health Management Information System (PHMIS) of The University of Washington. The purpose is to overcome the increased cost of healthcare for senior citizens. Not to be left behind, Ministry of Health of Malaysia as cited in (Jai Mohan 2004) have been looking for the most suitable HIS to be implemented in their hospitals which aim for paperless hospitals.

Other examples of health networks that have been deployed:

- The Arizona Telemedicine Program – initiated in July 1996.
- California Telehealth & Telemedicine Center
- Clallam County Hospital District 1
- Dakota Health Network, Avera St. Luke's Hospital, Aberdeen
- Dakota Telemedicine Network
- DownEast Telemedicine Network
- McKennan Health Service
- Mountain Plains Health Consortium, and
- NorthEast Telemedicine Network.

Shared goals of all these telehealth are

- Overcoming barriers of geographic such as remote and small population
- Limited telecommunication capacity, and
- Reduce time between diagnose and delivery of services

Each country which has HIS is doubling their effort to enhance their HIS capability and security. This is an ongoing process. The most important thing in any information system is the security concern. From the interviews conducted, I was acknowledged that there were three issues which are oftenly debated among the organizations within HIS. There are the kind of information should be shared, the amount of information and the

responsible security officer that appointed. Having said this, it should not be the reason for HIS not to be further implemented worldwide. Many effort been executed in order to find a solution for HIS threats.

The most common way to secure information is with the use of encryption and decryption. Besides that we have the identification and authentication process which allow authorized user to access the data only after they provide a correct identification such as password to access the system. There have been many improvements and modernized security feature introduced and implemented by the owner of the HIS in order to secure the information reside in their field.

As time evolved, the management of any IS has changed from central-management into distributed IS. With the new way of IS been carried out by the agent related in the distributed environment, there have been many researches performed to find the way of properly securing the information over the distributed environment. The most popular and promising way to manage enterprise wide system and distributed system is by implementing the policy based-management (Damianou February 2002).

As cited in the same paper, policy based management offers an ease in the complexity of managing multi-organizations in distributed environment where it capable of allowing heterogeneous security methods to be dynamically installed according to its precedence. In other words it's the policies that manage the overall system procedures. Taking policies to act as a manager of the overall procedures for all agents reside in the distributed network, comes with a list of policies. The most important policies are Access Control Policy. Other than that, they deploy Obligation Policy, Delegation Policy and many more. Again, as cited (Damianou February 2002), it explained on a one specific language for deploying these policies for widely distributed system, Ponder.

For the reader's information, the aim of this research is to propose a security language for policy based-management for Health Information System (HIS). So, the scope of this thesis is covering the policies that are related with the security concerns. Adding to that, DiHIS language tailored for policies exist in health institution only. The reason of not using the existing language such as The Authorization Specification Language (ASL) (Jajodia), A Language for Security Constraints on Objects (LaSCO) (Hoagland July

1998) and Ponder (Nicodemos Damianou 15 July 2002; Nicodemos Damianou 2001) will be discussed in the next section.

### 1.2 Current Situation

The issues of security and privacy are global issues. Having the new technology improved and introduced such as online banking, has increased the security concern among the citizens. If yesterday, a banking system was introduced, the security of the system must have been installed in order to gain the trust of the account holder. Without their trust, the system is useless. There will be a waste to invest a large amount of money creating the system but at the end the system is underuse.

Having said that, policy-based management has become a very promising solution to manage widely distributed system. (Damianou February 2002), (Sloman 1999). At the same time, more advanced security methods protections of the confidential information are introduced and it applies for different cases according to its importance and appropriately. This situation brings another issue to overcome which is how to correctly implement the suitable security method accordingly (Hedi Hamdi). This issue is not the main concern of this thesis, but the concern is more on having the correct and suitable language to implement the security policy resides within the distributed in HIS.

The Authorization Specification Language (Jajodia 4-7 May 1997 ) was written by Sushil Jajodia from George Manson University and friends. ASL was designed to tackle different types of authorization policies. The basis of this language is it assuming that there are a set of object that is allowed or denied to perform a series of actions. This language also has introduced the roles and groups elements instead of individual user. When a user is a member of one group, the user's privilege is entitle to the group's policies. This is better than assigning privilege individually that will takes up a lot of time. The language is arranged in the way the rule will be expressed at the left hand side while the condition is on the right hand side. The condition is the constraint that must be fulfilled in order for the rules to be executed (allowed or denied). As mentioned by them, it is yet to approve that this model can be applied in the representation and enforcement of complex system. Adding to that we finds this language is not so suitable for representing the policy based management for distributed system for the reason it doesn't

cover other important security policies resides within HIS such as information filtering policies and need to know problem. As cited in (Hedi Hamdi), ASL has failed to cater for the large systems due to the reason that it cannot group the rules into structures for reusability. Adding to that, ASL has no way presenting the delegation policy. More discussion about ASL will be in Chapter 4. There, we will be discussing the ability of ASL representing the clinical information system security model (Anderson 1997; Anderson Jan 1996; Anderson May 1996). The clinical information system security model is a security model introduced 1996 by Ross J. Anderson. This model will be discussed further later.

Beside the ASL, there is LaSCO which stands for Language for Security Constraint on Object. LaSCO security language is based on graphical view with annotation. The language applies the policies by showing a set of objects with a series of events. On the left hand side is the user object and the file object is at the right hand side. Both objects are connected with an edge where the event parameter is stated. In general, this language designed for security policies for access control. This language has been very good in representing the file system and it allows policies to be stated separately from the system. Just like ASL, LaSCO is lack of other important security policies that resides within distributed HIS such as delegation policy (Hedi Hamdi) which makes it inappropriate to be used for distributed HIS. In (Hedi Hamdi), they stated LaSCO weak in representing the auditing operations and control aggregation. And the language also left out another two important elements in securities which are confidentiality and integrity. The language has been used to represent the clinical information system security model and the result is in Chapter 4.

Another popular security language which has been the center of attraction in representing security policy is Ponder. Ponder is A Language for Specifying Security and Management Policies for Distributed System. Ponder was initiated in the first place to cater the problem of representing the policy based-management for widely distributed system. Ponder created as an object oriented languages and easy implementation with the tools created. The reason why Ponder inappropriate to represent the policy based management for distributed HIS is similar with the reason that have been stated earlier. Ponder is a language created to cater for all types of distributed system. For instance

financial institution, military environment and health care industry. Still there are areas within HIS not covered by the Ponder. As cited in (Hedi Hamdi), they raised the weakness of Ponder as unable to express several elements in communication security such as confidentiality and integrity. In Chapter 4, we used Ponder language to represent the clinical information system security model.

As have been mentioned several times, clinical information system security model (Anderson 1997; Anderson Jan 1996; Anderson May 1996) was created by Ross J. Anderson in 1996. The idea of initiating the model was raised by the British Medical Association (BMA) after big issues concerning the security of HIS. The issues of security have been risen up after the introduction of nationwide health networks. They expressed that there have been confusing on what should be protected and the justification. They also stated Bell-LaPadula security model is suitable for military whereas Clark-Wilson suitable for banking system. This left no suitable security model for HIS. Ross J. Anderson has been asked by BMA to come out with list of threats to clinical information security, the best security model for practices as well as the guidelines for HIS. The security model consists of 9 principles which stand for: access control, record opening, control, consent and notification, persistence, attribution, information flow, aggregation control and the trusted computing based. The detailed of 9 principles of the clinical information system security model will be presented in Chapter 4.

Here, we can conclude that none of existing security languages have the ability to represent the security policies reside within the distributed HIS completely. From this situation, we wants to bring the reader's attention to the problem statement that derives from issues discussed in this section.

### 1.3 Problem Statement

The current issues on security languages and formal specification languages have been stated and presented in the previous section. The main issue this research is trying to solve is the security policies issue concerning health care network.

*"A single policy simply cannot capture different protection requirements users may need to enforce on different data."*(Jajodia)

These days, they aim to create one method that can fit for all. That is not acceptable especially concerning security. Different institutions have different security concern and constraints. For instance banking system needed different protection if to compare with protection of health network system. Here is an example scenario, in banking system the most confidential information is the account details of the account holder. The name as well as the account number is not too strictly confidential since it is acceptable for other to know the account number for the reason depositing money into that particular account. The healthcare institution works the other way around. It is very crucial to hide the name and all personal information about a patient who has AIDS for instance. When they come to medical research, they would allow the diagnosis report of the patient to be used for research purposes as long as the real identity of the patient is not being revealed by the hospital. Although it seems that both institutions are protecting the confidential information about their customer or patient, in fact there are aspects that are unique only to one particular institution only. This issue lead to different policies to be implemented tailored for health care network.

In health care, there lies the most discuss issues that is need to know. Need-to-know principle was not included in the Anderson's model, as the BMA does not accept that 'need to know' is an acceptable basis for access control decisions further details found in (Anderson Jan 1996), (Anderson May 1996). However there might be where the need to know policy cannot be avoided. For instance a service provider such as social services offers its services conditioned by some information about the patient who applies such services.

There are two major problems concerning this policy. Firstly, who is authorized to decide about who needs to know in distributed services environment where responsibilities are distributed, and how to resolve the conflict between the patient consent and need to know? Further investigation will take place to find out whether the mandatory need to know exists.

Since there is no need to know without a task, we propose an approach based on associating the data with tasks and grant these tasks to performers rather than giving direct authorization to the secret data. The task could be in a form of an agreement between the information's owner and who needs to know (task's performer) and

consisting of full awareness about the task that requires the information, information size, release time, time of expire, and guaranty to restrict the use of this information by the specific task.

The term "need to know", used by the government and other organizations (particularly those related to the military or espionage), describes the restriction of sensitive data.

Under need to know policy, even if one has all the necessary official approvals (such as a security clearance) to access certain information, he would not be given access to such information unless one has a specific need to know; that is, access to the information must be necessary for the conduct of he's official duties.

As with most security mechanisms, the aim is to make it difficult for unauthorized access to occur, without inconveniencing legitimate access. This policy also aims to discourage "browsing" of sensitive material by limiting access to the smallest possible number of people.

It has been alleged that need to know policy (like other security measures) can be misused by some personnel who wish to refuse others access to information they hold in an attempt to increase their personal power, or to prevent unwelcome review of their work.

The need to know principle is at odds with most purposes of intelligence and research. While one part of an institution may have knowledge of some data, the rest of this institution as well as other institutions remain ignorant. Since experience shows that data shows its most valuable information only when freely connected, the need to know is in fact putting a limit on information that intelligence agencies can gather (even if there are no limits to the amount of data).

### 1.4 Research Question

Two research questions have been developed in an attempt specifically to discover the issue of security specification languages. The questions are:

- Which current security languages is the best to represent the Security Policy Model in Clinical Information System?
- How DiHIS security language is able to represent the Security Policy Model in Clinical Information System?

Answering this question has leaded to perform a number of literature reviews in order to obtain enough information before the proposed language can be created.

### 1.5 Objectives of Study

This research has outlined three objectives derived from the research questions of the study. The objectives are:

- To propose a security specification language for distributed HIS.
- To evaluate applicable of DiHIS security specification language with Security Policy Model in Clinical Information System.
- To validate the proposed language using a prototype as the case study.

Executing all three objectives of study requires full commitment from us to come out with a very concrete security specification language. Fulfilling all these three objectives means this research is successfully done.

### 1.6 Significance of Study

This research concentrates on HIS environmental situation. The important issues and problems of security within HIS are the major interest. One of the contributions of this research is proposing the solution for need to know policy.

Other issues on policies such as authorization and access control policy have also been tackled in this research by the proposed security specification language. This language extend the constraints of these policies in order to fit with the HIS circumstances.

Besides, the language is easy to use and the creation of tool and proof of this language are left for the future research.

### 1.7 Scope of the Study

This research concentrates on HIS environmental situation only. The issues raised within distributed HIS policy based-management implementation have been the major concern of this research.

The literature review done has helped us to identify the strength and weakness in current situation. We proposed the possible solution due to the identified weaknesses.

Besides that, this research is applying Security Policy Model in Clinical Information System (Anderson Jan 1996; Anderson May 1996) as the main comparison of applicability of the proposed security languages with others. This model chosen because it was initiated at the time of emerging health care centralized system to distributed system. This model listed all the basis requirements that should be adhered by any organization who wish to employ distributed HIS.

The policies covered in this research are access control policies, authorization policies, obligation policies, delegation policies, refrain policies, transaction policies, and need to know problem.

After that, the thesis proceeds with representing the language into a prototype of distributed HIS as case study to validate the proposed language.

**1.8 Methodology**

In this section, we are going to explain the step she has taken in completing the research.

We commenced with the literature review of others security languages to look for the ways these languages construct the syntax and semantics. The languages which have been studied are ASL, LaSCO and Ponder. These languages are the security languages and the most related work with the objectives of this research.

Besides this three security languages, we has performed same literature review on formal specification languages such as Z Languages(Spivey 1992) and VDM-SL (Kainhofer 2000). The importance of identifying various numbers of languages is for us to get a clear picture on how to create a specification language correctly.

After that, we create the DiHIS – security specification language with the model overview, along with the syntax and the semantic of the language. A list of symbol used in the language shown in a table for a better understanding of the readers.

We also has done comparison the applicability of the DiHIS language with three others security languages which have been stated earlier. The clinical information system security model (Anderson May 1996) created by Ross J. Anderson has been chosen as the state of comparison. This model has been chosen for the reason this model initiated in the first place to overcome the confusion rise within health network system when it was first introduced and implemented. This model has become the basis need for any government

bodies who are interested to initiate its own health network system. The result of the comparison intended to show that DiHIS specification language is better than the three other security languages.

In order to verify the proposed language, we come up with a prototype of distributed HIS. We present all the possible policies that are needed in all kinds of possible situation that could happen within the distributed HIS.

### 1.9 Thesis Organization

Chapter 2 presents literature review and related works that have been performed by others researchers. The chapter starts with the discussion of existing security models and afterwards it narrowed to the discussion of several examples of security languages.

Chapter 3 present essential issues that are extremely important to tackle in order to building distributed HIS.

Chapter 4 presents the proposed language; DiHIS security specification language for distributed system is discussed. This chapter presents the language overview as well as the construction of the language. After that, it will proceed with showing the comparison of DiHIS with other security languages representing Security Policy Model in Clinical Information System.

Chapter 5 presents the prototype of distributed HIS as case study presented and discussed in details. Each of the policies involved within the connection is presented. Afterwards, the applicability of DiHIS security specification language to represent those policies is tested. This chapter ends with discussion of the case study.

Chapter 6 presents the overall conclusion of this research. The discussion about future work ends this thesis.

# CHAPTER TWO

## LITERATURE REVIEW

A great deal of works has been done in the security models and languages area. Most of them focus on developing and creating general security models that can be applied to all fields. Health care system, business, and banking are some of the fields that the aforesaid models had successfully been applied to. Many researchers had focused on applying and enforcing the security mechanisms into the health care systems using Ponder language which is an object oriented security language initiated for deploying the policy based management in distributed systems. However, need to know policy which is an important issue in access control and assigning authorization in health care system hadn't been covered in Ponder language as declared in this chapter. In contrast DiHIS security specification language successfully manages to overcome need to know- problem. Several different works that is strongly related to this research have been conducted as below.

## 2.1 Security Policy

Several goals and elements of an organization's computer systems usually formally/ informally defined using computer security policy. Organizational policies usually applied to enforce the security policies. To ensure the computer system security, technical implementation is highly supported by the security researchers. Moreover, security concept could be categorized into three different parts which are Confidentiality (Bell LaPadula model), Integrity (Biba model), and Availability.

### 2.1.1 Anderson's Security Policy Model for Clinical Information System

The security policy model was initiated by Ross J. Anderson in 1996 as requested by the British Medical Association (BMA). BMA requested Anderson to come out with security policy model specifically for clinical information system since at that time there is no security models that are suitable for clinical information system. At that time, there have been many confusion and issues rose from the deployment of clinical information system. They have been questioning what the threats to the personal information are and how to protect this information (Anderson May 1996). Anderson has come out with 9 principles of security clinical information system which has been specially initiated by the doctors by means of motivated by medical ethics. The model consists of access control, record opening, consent and notification, persistence, information flow, attribution and aggregation control. Below is the discussion on the model.

**Access control**

**Principle 1**: *Each identifiable clinical record shall be marked with an access control list naming the people or groups of people who may read it and append data to it. The system shall prevent anyone not on the access control list from accessing the record in any way.*

Each subject may have access to certain objects which may be stored by subject or object. So, according to the above principle, two types of objects can be categorized according to the authority of accessing and modifying the records. The first is the capabilities which can be stored by subject for an instance clinicians, while the second is the access control list that stored by object for instance patients, this access control list clarify who can do

what. For example X may be capable of reading Z's records. On the other hand and for declaring the access control list, the Y could be the one to do it.

Thus, instead of individual names, X and Y could be represented by Swaffham. Swaffham represents the group name. The example had been done by the development of Care Community which has involved doctors, nurses, and social services staff. At the start of the assessment for the information to be shared, written permission has been achieved. This is how the patient may come to know to whom the record is assigned.

Assigning an access control to a group of people may seem a good solution but this method is associated with more complex situation. However, groups usually involve a large number of people, just like a hundred of nurses that possibly may be assigned on duty to a ward. Thus the following rule could be added: nurses on duty at one particular time or nurses on duty in the same ward of the patient. For instance, normally the real case is the user could be coping with various kinds of groups, nurse, doctor, patient, trainer, trainee, manager, and consultant etc. This complexity has to be handled.

On another hand, ad hoc method which means to give up on a consistent policy and just carry on with current chaos should be avoided. That could be done using provision (a clause of condition in a contract).

Additionally, sharing the same password for a group is not advisable, such as the same password sharing for a group of nurses at the same ward.

However, since the number of patients that a doctor may attend is mostly larger than the number of doctors which attends to one patient, hence action can be performed by clinician could be as follows:

- Read
- Add information (append data to it)
- Delete

So a clinician can access the record for a particular patient and then listed in the access control list only for this record. Conversely, a doctor may have the access to many records.

**Record Opening**

**Principle 2**: *A clinician may open a record with herself and the patient on the access control list. Where a patient has been referred, she may open a record with herself, the patient and the referring clinician(s) on the access control list.*

For the second principle, Anderson assumed that one patient may have multiple types of records just as:

- All clinician may access a general record
- Some records cannot be accessed by many, especially a highly sensitive record of a treatment.
- All of the staff may have the access to special record, for example heart disease, the patient may take a summary of such kind of diseases on an emergency medical card for faster and easier treatment. The card may contain many records with different access control level.

**Control**

**Principle 3**: *One of the clinicians on the access control list must be marked as being responsible. Only she may alter the access control list, and only she may add other health care professionals to it.*

The third principle of this model related with the second principles. In previous principle, it suggest only authorized person can access the record meanwhile this principle promote the importance of controlling access to the record. Anderson suggested appointing one clinician that involved within the access control to become a responsible clinician. Enforcing the informed consent and works related with assigning access control list will be the responsibilities of this responsible clinician. Having said this, there is still issue rise related with access control.

Need to know is one issue that is continuously been debated and discussed by the patients concerning about their sensitive clinical records where they disagree with the administrative personal who claimed they need to access certain clinical records in order to perform their job smoothly. Usually this situation occurs in time of emergency such as epidemic.

In reality, when two organization has agreed to share clinical records (For instance social worker, lawyer, police, security service officer, insurance company, and employer), it always done in hardcopy form. They prefer paper for the rationale is a lot easier to impose the credential by the owner of the records. Whereas they found using softcopy records did not provide the same safe feeling as using the paper form.

From our own experience, using internet banking offers a lot more convenience than traditional way queue at the bank. This technology reduces waiting time, easier to transfer money and reduce the risk been robbed from carry a lot of money with self. The most important thing needed from the provider of the system is to provide the optimum protection that will lead to gaining trust from the customer. The same apply toward health care information system.

**Consent and notification**

**Principle 4**: *The responsible clinician must notify the patient of the names on his record's access control list when it is opened, of all subsequent additions, and whenever responsibility is transferred. His consent must also be obtained, except in emergency or in the case of statutory exemptions.*

This principle encourages the concept of notification to the patient and obtaining their consent for any changes made by the clinician to their clinical records. The changes are adding, deleting of clinicians that have access control list to the patient clinical records. Adding to that in case of the patient referred to another clinics or hospital, the clinician at the referred clinic or hospital will be added to the patient access control list too. This situation also must be informed by the responsible clinician to the patient in advance.

Information breaching frequently occur during in case of emergency. During emergency, the health record is shared between the emergency unit's staff and the GP. The GP is a medical practitioner who gives primary care and specializes in family medicine . A general practitioner treats acute and chronic illnesses and provides preventive care and health education for all ages and both sexes) For instance a patient X meets an accident on the road. X treated by the emergency unit which requires sufficient information to saves X's life. Let assume an authorized person made a phone call to obtain follow up news about X. It's the hospital responsibility to ensure the validity of the caller status.

Since allowed call must between staff in the emergency unit and in the ward to exchange clinical records, an authorized call can be identify by calling back to a number in Medical Register.

The significant of notification comes from the fact that it can offer an end-to-end audit which is unsusceptible to management capture of auditors or regulators. Whenever an access for the patient personal health information record being requested by hospitals' staff, the callback control will not be effective (because that person is a hospital staff) but still the reason of accessing the record related with patient. Then, notifying the patient ensures the attack can be detected and investigated.

When it is related with legal duty, the notification must be performed anyway (For instance even though it will cause the suspect to flee, intimidate witnesses).

There also question on how frequent to notify the patient. Current practices notify the patient annually by letter unless a suspicious or violation pattern of activity has been detected. Some clinicians discuss with the patient how the notification will be sent. (For instance if using letter, their secret about health will be known to others)

When the relationship patient-clinician has come to an end (For instance patient died, go abroad and the problem has been dissolved), the question of where the information will be kept arose. It has been suggested that the Data Protection registrar have custody of all the "dead" electronic records. However this raises a question; who will watch the watchman?

Last but not least, there must be an effective complaint procedures which will result in offenders will be punished.

**Persistence**

**Principle 5**: *No-one shall have the ability to delete clinical information until the appropriate time period has expired.*

This principle deals with the deletion of old records. Each record has been allocated its own lifetime according to the type of disease. Most records are required to be kept for 8 years. Clinical records of cancer disease patient obligated to be kept for the patient's lifetime. Records of genetic diseases must be kept longer (for future reference) some

example on the duration records allowed to be saved inside the system before it asked to be deleted.

There are also laws on deciding how long time before the record will be completely deleted. But, this paper stated that these rules or law are still not fully worked out and suggest the Principle 5 which covers a number of outstanding issues.

- This policy allow destruction of old record but does not mandate it; there are many cases in which it is appropriate to keep records for longer that the law requires (For instance chronic illness).
- 6th principle of the Data Protection Act states that "personal information shall not be held for longer than is necessary". This may mean that once the clinician is no longer the primary record holder then the record should be destroyed. But, by doing this, she may wish some assurance that it can be made available if necessary (For instance in the event of lawsuit);
- Patient consent changing. They might insist that the record be destroyed. Perhaps; such cases will be dealt by transferring the primary record to a clinician of the patient's choice for the rest of the statutory period.
- With temporary copies of records, the appropriate time period will shorter. For instances:
    - Night time deputizing services, the condition that all copies of records b deleted within a set period of time.
    - Copies of record held by a safe-heaven, an auditor or researcher; consent to record sharing for research should be renewed every 5 years (so that copies of records made by researchers should persist no longer than that).

This kind of control has impact on the aggregation control. Preserving records is not completely straightforward; we do not want mistaken or inaccurate info to be acted on as this will destroy the integrity value. However we do not want traceless erasure of mistake as it would destroy the record's evidential value. So, information should be updated by appending rather than by deleting and the most recent versions brought first to the clinician attentions. Deletion should be reserved for records that are time expired.

**Attribution**

**Principle 6**: *All accesses to clinical records shall be marked on the record with the subject's name, as well as the date and time. An audit trail must also be kept of all deletions.*

Ensuring all record accesses (read, append or delete) are correctly attributable.

Audit trail enables the state of records as it was at any time to be reconstructed and all changes to be attributable. Each action performed is kept inside the log. So that in case of information breaches can be traced and punished. The deletion logged so that the deliberate destruction of incriminating material can be attributed. Some application has strict rules attribution requirements. There are also attribution requirements that are rarely invoked. So, this requirement usually supported with manual mechanism.

**Information Flow**

**Principle 7**: *Information derived from record A may be appended to record B if and only if B's access control list is contained in A's.*

When two records with different access control lists correspond to the same patient, then the only information flow permissible without further consent is from the less to the more sensitive record.

When two records with different access control lists correspond to the same patient, the hard question is whether existence of the sensitive record will be flagged in the other one. If existence hidden information is flagged, whether explicitly or by conspicuous, the conclusion can easily drawn. For instances:

First problem:

A doctor removes health records from the computer system whenever the patient was diagnosed with cancer (the records being remove because its confidentiality). The result was whenever an insurers and pension funds saw a blank record; they knew that with high probability the subject was a cancer sufferer.

Second problem:

A psychiatrist outpatient goes for an AIDS test and request that result kept as secret. Before the result known, the stress causes a breakdown and his psychiatrist marks him as no longer competent to see his records. However, the psychiatrist is unaware of the test

and does not tell the STD clinic of the patient's new status. The solution? This paper stated that it is not possible having a world readable register of which patients are currently not competent (For instance mental incapacity), is both confidential and a function of circumstances.

Related problem (with second problem):

A person suffers Munchausen's syndrome hard to detect and manage.

Explanation:

Munchausen's syndrome is a person who exaggerates or creates symptoms of illnesses in themselves in order to gain investigation, treatment, attention, sympathy, and comfort from medical personnel. Their "illnesses" whose symptoms are either self-induced or falsified by the patient. For example, they may inject a vein with infected material, causing widespread infection of unknown origin, and as a result cause lengthy and costly medical analyses and prolonged hospital stay. Patients with Munchausen syndrome are aware that they are exaggerating.

Visible flag is been discuss in UK. This shows that visible flag must be discuss and agreed by the clinicians so that the action won't cause harm in the future to the hospitals of to the patient.

They suggested system developers should give carefully consideration to the propagation of sensitivity properties through dependent records, and to the effect of the system integrity.

The second recommendation was there a need for a mechanism for dealing with the release of data that have been made anonymous should require a deliberate act by the responsible clinician and should be logged.

**Aggregation control**

**Principle 8**: *There shall be effective measures to prevent the aggregation of personal health information. In particular, patients must receive special notification if any person whom it is proposed to add to their access control list already has access to personal health information on a large number of people.*

Brief explanation about aggregation control this is in term of technicality when transferring information between sender and receiver.

Reliable data transmission protocols between a sender and a receiver often use feedback from receiver to sender to acknowledge correct data delivery. Such feedback is typically sent as control messages by receiver nodes. Since sending of control messages involves communication overhead, many protocols rely on aggregating a number of control messages and sending them together as a single packet over the network.

On the other hand, the delays in the transmission of control messages may reduce the rate of data transmission from the sender. Thus, there is a basic tradeoff between the communication cost of control messages and the effect of delaying them.

We develop a rigorous framework to study the aggregation of control packets for multicast and other hierarchical network protocols. We define the multicast aggregation problem and design efficient online algorithms for it, both centralized and distributed (Sanjeev Khanna 2002).

In Anderson's research paper, he stated that notification very helpful in use of access control list but not enough to prevent the aggregation threats. The reason he stated by looking at below example.

Some hospital's system contains personal health information on a million or more patient, with all users having access. For instance having 2000 staff accessing a million records is bad enough and if there was the prospect of 200 such hospitals connected together, giving 400 000 staff access to the hospital records of the most population, is unacceptable.

So, hospital systems which give all clinicians access to all data should not be connected to the network.

However, there have been a mechanism to able clinicians accessing records from outside their own team (manually) but this requires carefully design. Because there could be some corrupt member (the corrupt member falsely claims that a patient has self-referred while on holiday and asks for a copy of the record to be sent).

Control methodology:

There are two types of aggregation control:

- Primary control ;Notification
    - Get feedback from the patient
- Secondary control; Keep a count that has access what record outside their team.

- There are 2 things that need to be allocated effectively or carefully chosen; the location of the count and the person responsible for action on it (For instance healthcare unions and clinical disciplinary bodies).

Current practice for records used on research purposes; records made anonymously by replacing name with NHS numbers and diagnoses with Red codes. But making data anonymous is hard, especially if it contains linkable information; id an attacker submit database queries such as " show me the records of all females aged 35 with two daughters aged 13 and 15 both whom suffer from eczema", then he can identify the individuals. Current way to prevent this problem called "statistical security". This has done by limit the linkage, and techniques for preventing inference.

**The trusted computing base**

**Principle 9**: *Computer systems that handle personal health information shall have a subsystem that enforces the above principles in an effective way. Its effectiveness shall be subject to evaluation by independent experts.*

At this section they first define the word "trust". After that, he relates them with the concept of trusted computing. If in real life trust means that we rely on that person to do something or not to do certain things. At this kind of relationship, it can be applied for computer design.

The trusted computer base of a clinical information system may include:

- computer security mechanisms to enforce user authentication and access control,
- communications security mechanism to restrict access to information in transit across network,
- statistical security mechanisms to ensure that records used in research and audit do not posses sufficient residual information for patients to be identified, and
- Availability mechanism such as backup procedures to ensure that records are not deleted by fire or theft.

This paper also suggests that it is not sufficient enough to rely on the assurance of "equipment salesman" that their product is secure but must be checked by a competent third party. In Europe, they practice independent evaluation, under which national

computer security agencies license commercial laboratories to carry out security evaluations. Other countries which have similar practice are Australia, Canada and USA.

We found that Anderson's 9 Principles for Security Model Clinical Information is a complete model at the time it was initiated. The principles cover all aspect of information security that should be used by any organization that wishes to deploy DISTRIBUTED HIS. But, now day, there are increasing deployment of connection in distributed environment. This new concept required more dynamic features with little update (Leonidas Lymberopoulos 2002).

For instance, User-Defined Rules; the system should be flexible enough to allow adding new rules by the administrator with minimal updates.

Besides the ability to add new rules into the policy, there's a need for flexibility of adapting to changes in the organization.

We found that the third principle supposedly placed earlier before the second principle. The reason is that in Principle 2 it stated about the access control list that already created. It means that it must already have the responsible clinician that manages the access assigning which clinician to what clinical record. Because when a system is to be implemented, the security features must be installed before the system implemented in real world. Installing the security after the system been implemented is not acceptable. Moreover, this policy not applicable for distributed health system. It failed to support the policies badly needed in order to ensure the protection for all agents, maybe because this model was initiated in 1996 where the distributed health system is not applied yet.

In our research, we are presenting a language for policy based management for health information system. This language intended to represent the above policy as well as support the involved distributed policy for HIS.

**2.2 Security Policy Models**

Designers of military and banking systems can refer to Bell-LaPadula and Clark-Wilson respectively that spells out clear and concise access rules about what should be protected and why (Anderson Jan 1996). There also a number of other security policy models presented as a means of clearing the confusion as well as the guidelines of how the protection should be executed.

A non-disclosure agreement (NDA) (often known outside of the United States as a confidentiality agreement; occasionally called a confidential disclosure agreement or CDA, or secrecy agreement), is a legal contract between at least two parties that outlines confidential materials or knowledge the parties wish to share with one another for certain purposes, but wish to restrict access to. It is a contract through which the parties agree not to disclose information covered by the agreement. An NDA creates a confidential relationship between the parties to protect any type of confidential and proprietary information or a trade secret. As such, NDA protects non-public business information.

NDA are commonly signed when two companies or individuals are considering doing business and need to understand the processes used in each other's business for the purpose of evaluating the potential business relationship. NDAs can be "mutual", meaning both parties are restricted in their use of the materials provided, or they can restrict the use of material by a single party.

It is also possible for an employee to sign an NDA or NDA-like agreement with an employer. In fact, some employment agreements will include a clause restricting employees use and dissemination of company owned "confidential information." NDA are used in the IT field, and are often given directly prior to taking a certified exam.

### 2.2.1 Bell LaPadula Model

In this formal model, the entities in an information system are divided into subjects and objects. The notion of a "secure state" is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby inductively proving that the system satisfies the security objectives of the model. The Bell LaPadula Model is built on the concept of a state machine with a set of allowable states in a system. The transition from one state to another state is defined by transition functions.

A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a security policy. To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object (more precisely, to the combination of classification and set of compartments, making up the security level) to determine if the subject is authorized for the specific access mode.

The clearance/ classification scheme is expressed in terms of a lattice. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties:

- The Simple Security Property states that a subject at a given security level may not read an object at a higher security level (no read up).
- The *-property (read star-property) states that a subject at a given security level must not write to any object at a lower security level (no write down).
- The Discretional Security Property uses an access matrix to specify the discretionary access control.

The transfer of information from a high-sensitivity paragraph to a lower-sensitivity document may happen in the Bell LaPadula model via the concept of trusted subjects. Trusted Subjects are not restricted by the *- property. Entrusted subject are. Trusted Subjects must be shown to be trustworthy with regard to the security policy.

With Bell LaPadula, users can create content only at or above their own security level (Secret researchers can create Secret or Top Secret files but may not create Public files): no write down. Conversely, users can view content only at or below their own security level (Secret researchers can view Public or Secret files, but may not view Top Secret files): no read up.

The Bell LaPadula model explicitly defined its scope. It did not treat the following extensively:

- Covert channels. Passing information via pre-arranged actions was described briefly.
- Networks of systems. (Later modeling work did address this topic)
- Policies outside multilevel security. Work in the early 1990s showed that MLS is one of the versions of Boolean policies, as are all other policies.

Strong * Property

The Strong * Property is an alternative to the *-property in which subjects may write to objects with only a matching security level. Thus, the write up operation permitted in the usual *-property is not present, only a write to same operation. The Strong * Property is usually discussed in the context of multilevel database management systems and is motivated by integrity concerns. This Strong * Property was anticipated in the Biba

model where it was shown that strong integrity in combination with the Bell LaPadula model resulted in reading and writing at a single level.

Tranquility Principle

Tranquility principle of Bell LaPadula model states that the classification of a subject or object does not change while it is being referenced. There are two forms to the tranquility principle:

- The "principle of strong tranquility" states that security levels do not change during the normal operation of the system.
- The "principle of weak tranquility principle" states that security levels do not change in a way that violates the rules of a given security policy.

Another interpretation of the tranquility principle is that they both apply only to the period of time during which an operation involving an object or subject is occurring. That is, the strong tranquility principle means that an object's security level/ label will not change during an operation (such as read or write); the weak tranquility principle means that an object security level/ label may change in a way that does not violate the security policy during an operation.

Limitation of this model:

- Restricted to confidentiality
- No policies for changing access rights; a complete general downgrade is secure; intended for systems with static security levels.
- Contains covert channels: a low subject can detect the existence of high objects when it is denied access.
- Sometimes, it is not sufficient to hide only the contents of objects. Their existence may have to be hidden, as well.

### 2.2.2 Biba Model or Biba Integrity Model

Biba model developed by Kenneth J. Biba in 1977 is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in level ranked higher that the subject, or be corrupted by data from a lower level than the subject. In general the model was

developed to circumvent the weakness in the Bell LaPadula model which only addresses data confidentiality.

In general, preservation of data integrity has three goals:

- Prevent data modification by unauthorized parties
- Prevent unauthorized data modification by authorized parties.
- Maintain internal and external consistency (For instance. data reflects the real world)

This security model is directed towards data integrity only (rather than confidentiality) and is characterized by the phrase: "no write up, no read down". This is in contrast to the Bell LaPadula model which is characterized by the phrase "no write down, no read up". However data integrity is not enough for comprehensively security representation. Besides, two security concepts are missed in the Biba model, which are Availability and Confidentiality.

In the Biba model users can only create content at or below their own integrity level (a monk may write a prayer book that can be read by the commoners, but not one to be read by the high priest.) Conversely, users can only view contents at or above their own integrity level (a monk may read a book written by the high priest, but may not read a pamphlet written by a lowly commoner).

The Biba model defines a set of security rules similar to the Bell LaPadula model. These rules are the reverse of the Bell LaPadula rules:

- The Simple Integrity Axiom states that a subject at a given level of integrity may not read an object at a lower integrity level (no read down).
- The * (star) Integrity Axiom states that a subject at a given level of integrity must not write to any object at a higher level of integrity (no write up).

### 2.2.3 The Graham-Denning Model

The Graham-Denning model is a security model that shows how subjects and objects should be created and deleted. It also addresses how to assign specific access rights. This model addresses the security issues associated with how to define a set of basic rights on how specific subjects can execute security functions on an object. As cited in Graham's approach, the model has eight basic protection rules that outline:

- How to securely create an object
- How to securely create a subject
- How to securely delete an object
- How to securely delete a subject
- How to securely provide the read access right
- How to securely provide the grant access right
- How to securely provide the delete access right
- How to securely provide the transfer access right

Taking into consideration the above model, security models have to apply to some-if not all- Graham-Dennings' rules since it highlights significant points for assigning authority and privacy, therefore some of the aforesaid rules will be applied to the security specification language.

### 2.2.4 Clark-Wilson Integrity Model

This model provides a foundation for specifying and analyzing an integrity policy for a computing system. This model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. An integrity policy describes how the data items in the system should be kept valid from one state of the system to the next and specifies the capabilities of various principals in the system.

The model defines enforcement rules and certification rules. The model's enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the notion of a transaction.

- A well-formed transaction is a series of operations that transition s system from one consistent state to another consistent state.
- The integrity policy addresses the integrity of the transactions.
- The principle of separation of duty requires that the certifier of a transaction and the implementer be different entities.

The model contains a number of basic constructs that represent both data items and processes that operate on those data items. The key data type in this model is a Constrained Data Item (CDI). An Integrity Verification Procedure (IVP) ensures that all

CDIs in the system are valid at certain state. Transactions that enforce the integrity policy are represented by Transformation Procedures (TPs). A TP takes as input a CDI or Unconstrained Data Item (UDI) and produces a CDI. A TP must transition the system from one valid state to another valid state. UDIs represent system (such as that provided by a user or adversary). A TP must guarantee (via certification) that it transform all possible values of a UDI to a "safe" CDI.

The rules

At the heat of the model is the notion of a relationship between an authenticated principle for instance user) and a set of programs (For instance TPs) that operate on a set of data items (For instance UDIs and CDIs). The components of such a relation, taken together, are referred to as Clark-Wilson Triple. The model must also ensure that different entities are responsible for manipulating the relationships between principals, transactions, and data items. As short example, a user capable of certifying or creating a relation should not be able to execute the program specified in that relation.

The model consists of two sets of rules: Certification Rules (C) and Enforcement Rules (E). The nine rules ensure the external and internal integrity of the data items. To paraphrase these:

C1 – When an IVP is executed, it must ensure the CDIs are valid.

C2 – For some associated sets of CDIs, a TP must transform those CDIs from one valid state to another.

Since we must make sure that these TPs are certified to operate on a particular CDI, we must have E1 and E2.

E1 – System must maintain a list of certified relations to ensure only TPs certified to run on a CDI change that CDI.

E2 – System must associate a user with each TP and sets of CDIs. The TP may access the CDI on behalf of the user if it is "legal".

This requires keeping track of triples (user, TP, {CDIs}) called "allowed relations".

C3 – Allowed relations must meet the requirements of "separation of duty".

We need authentication to keep track of this.

E3 – System must authenticate every user attempting a TP. Note that this is per TP request, not per login.

For security purposes, a log should be kept.

C4 – All TPs must append to a log enough information to reconstruct the operation.

When information enters the system it need not to be trusted or constrained (For instance. UDI). We must deal with this appropriately.

C5 – Any TP that takes a UDI as input may only perform valid transactions for all possible values of the UDI. The TP will either accept (convert to CDI) or reject the UDI.

Finally, to prevent people from gaining access by changing qualifications of a TP:

E4 – Only the certifier of a TP may change the list of entities associated with that TP.

Generally, Security Modes refer to information systems security modes of operation used in MAC system. Often, these systems contain information at various levels of security classification. The mode of operation is determined by:

- The type of user who will be directly or indirectly accessing the system.
- They type of data including classification levels, compartments, and categories that are processed on the system.
- The type of levels of users, their need to know, and formal access approvals that the users will have.

**Dedicated Security Mode**

In this mode of operation, all users' must have:

- Signed NDA for ALL information on the system.
- Proper clearance for ALL information on the system
- Formal access approval for ALL information on the system
- A valid need to know for ALL information on the system

In summary, all users can access ALL data.

**System High Security Mode**

In this mode of operation, all usesr must have:

- Signed NDA for ALL information on the system.

- Proper clearance for ALL information on the system
- Formal access approval for ALL information on the system
- A valid need to know for SOME information on the system

In summary, all users can access SOME data, based on their need to know.

**Compartment Security Mode**

In this mode of operation, all users must have:

- Signed NDA for ALL information on the system.
- Proper clearance for ALL information on the system
- Formal access approval for SOME information they will on the system
- A valid need to know for SOME information on the system

In summary, all users can access SOME data, based on their need to know and formal access approval

**Multilevel Security Mode**

In this mode of operation, all users must have:

- Signed NDA for ALL information on the system.
- Proper clearance for SOME information on the system
- Formal access approval for SOME information they will on the system
- A valid need to know for SOME information on the system

In summary, all users can access SOME data, based on their need to know, clearance and formal access approval.

**2.3 Security Policy Languages**

To represent a concrete policy especially for automated enforcement of it, a language representation is needed. There exist a lot of application specific languages that are closely coupled with the security mechanisms that enforce the policy in that application. Domain Type Enforcement-Language, are independent of the concrete mechanism.

Security policy languages are languages that created for representing the policies. Because of the common usage, policies are written using natural English writing. This is because the policies created by man and they wrote in the language that they understood.

This language cannot be understood by the computers which only understand digits 1 and 0. So, there is a need for the development of security language which can turn the policies into a language that computer can understand for automated execution.

Multi-organization Services Environment and Collaboration Issue

Despite some form of cross-organization access control such as Principle 4 that requires informing the patient about any addition to his record access control list or those concerning the auditing aspect (For instance, Principle 6). In general, the issue of sharing clinical information including collaboration activities with other agencies such as police, social services or the education authority were not clearly considered (O'Conor 15 May 1999). One possible reason could be that these principles derived from centralized system idea at least from responsibilities and ownership point of view. Below are summaries of Security Specification Languages which are generally assisting implementing policy for distributed management.

### 2.3.1 Task Based Access Control (TBAC) model

Sandhu and Thomas explained in (Sandhu August 11-13, 1997) how access control can be restricted using the active security model concept. The active security model here means the security enforcement from the activity or tasks performed. Differ from the traditional paper based authorization process, TBAC provide tighter just-in-time need-to-do permissions in application environment. TBAC has ability to granting, usage tracking, and revoking permission in automated way.

### 2.3.2 The Ponder Policy Specification Language

Ponder is a declarative, object-oriented language for specifying security and management policy for distributed object system.(Nicodemos Damianou 2001) Specifying security policies that map onto various access control implementation mechanisms for firewalls, operating systems, databases and Java. It supports obligation policies that are event triggered condition-action rules for policy based management of networks and distributed systems. Ponder can also be used for security management activities such as registration of users or logging and auditing events for dealing with access to critical resources or security violations. Key concepts of the language include roles to group policies relating

to a position in an organization, relationships to define interaction between roles and management structures to define a configuration of roles and relationship pertaining to an organizational unit such as department. These reusable composite policy specifications cater for the complexity of large enterprise information systems. Ponder is declarative, strongly-typed and object-oriented which makes the language flexible, extensible and adaptable to a wide range of management requirements. (Nicodemos Damianou 2001)

### 2.3.3 Simplifying Network Administration using Policy based-Management

Verma in (Verma March 2002)stated that the heart of policy management lies in the policy transaction logic: how the policies will be represented and managed. The policy transformation logic module validates the information provided in the high level policies and transforms them into the configuration of devices in the network. The validation process must incorporate syntactical checks as well as semantic checks. The semantic validation of high level-policies consists of various types of checks:

- Bound checks – validate that values taken by an attribute in the policy specification are within specific limits determined by the network administrator.
- Relation checks – validate that the value taken by any two parameters in the policy specification satisfy a relationship determined by the specific technology.
- Consistency checks – validate that any two policies defined by the administrator do not conflict with each other.
- Dominance checks – checks for "unreachable policies": policies defined by an administrator that will never become active in the network because they are rendered ineffective by the definition of other policies.
- Feasibility checks – ensure that the set of policies desired by an administrator for a network are feasible in the operating environment provided by the network.

**The policy representation**

The policies required for network management can be specified in many different ways. Among the researchers who are involved in specifying policies, multiple approaches for policy specification have been proposed. These approaches range from an interpretation

of policies as programs to an interpretation of policies as simple entries in a directory or databases.

From a human input standpoint, the best way to specify a high-level policy would be in the terms of natural-language input. Although these policies are very easy to specify, the current state of natural-language processing, a special area within the field of artificial intelligence, needs to improve significantly before such policies can be expressed in this manner.

The next approach is to specify policies in a special language that can be interpreted by a computer. This map a policy to a piece of software that can be executed by a computer-interpretable program, it is possible to execute them. However, in general it is quite difficult to determine if the policies specified by two different programs are mutually consistent.

A simpler approach is to interpret the policy as a sequence of rules, in which each rules is in the form of simple condition-action pair (in the if then else format). The rules are evaluated on specific triggers, such as the passage of time or the arrival of a new packet within the network. If rule's condition is true, then the action is executed.

An alternative specification of policies is to represent them simply as entries in a table. The table consists of multiple attributes. Some of these attributes constitute the condition's part, and others constitute the action part. Different types of tables need to be specified if the condition components or action components of different rules vary. Such a tabular representation is rich enough to express most of the policies that can be specified with rule-based notation. Furthermore, it is easier to analyze for dominance and consistency.

### 2.3.4 Policy Driven Management for Distributed Systems

Sloman in (Sloman 1994) describes the two classes of policy – authorization policies define what a manager is permitted to do and obligation policies define what a manager must do. Policies specified as objects which defines a relationship between subjects (managers) and targets (managed object). Domains used to group the objects to which a policy applies. Policy objects also have attributes specifying the action to perform and constraints limiting the applicability of the policy. This paper also show how a number of

policies can be modeled using these objects and briefly mention issues relating to policy hierarchy and conflicts between overlapping policies.

### 2.3.5 Policy- Based Security Management for Federated Healthcare Database (or RHIOs)

Rafae Bhatti and friends in (Rafae Bhatti 2006) addresses the problem of the security management requirement for RHIOs from the perspective of database system principles. We stated each organization (inside RHIO) has specific policies for the access to data and the greatest effort in building a RHIO is in establishing the policy level agreements. This paper present a context aware-aware policy-based system to mitigate the security policy implementation challenges. The two parts are describes as implemented, one a set of disclosure and privacy policies for EHRs using a requirements specification based on a set of uses cases for the HL7 Clinical Document Architecture (CDA) standard proposed by healthcare informatics community. Two, this paper presents a context-aware policy specification language that allows encoding of CDA-based requirements use-cases into privacy and disclosure policy rules. This language enables specification and enforcement of privacy-aware access control for federated healthcare information across traditional organization. New policy should restrict the access to particular record, location condition, and time condition. The policy must address the disconnection of the user from the access right when the condition is no longer satisfied.

This paper set permission role (a role that allow to do what action to what thing). Then it has a set of permission engaged with the operation. These two different parts declared differently. So, when one object put inside one role of permission. Then, that object will have the permission to perform action referring to the permission role match with the permission operation.

### 2.3.6 Role Based Access Control (RBAC)

This policy involves the notion of roles embodying a collection of permissions, such that users obtain permission by being assigned to the roles instead of being directly assigned those permissions (Lupu; Sandhu 1996; Lupu 1997). RBAC suitable for authorization. In RBAC, users are assigned to roles, and roles are associated with privileges that can be exercised by activating a role. However, RBAC alone is no sufficiently expressive for

information governance on the Spine (Becker 2006). The reason stated by us is the process of role membership and privilege assignments are subject to multitude of rules. These rules come in different variants and not sufficient enough to extend RBAC by a fix number of built-in constraints. Since permission is not directly assignable to individual users, it is impossible to use RBAC to differentiate users with practically different capabilities in the system. Another insufficiency in the RBAC model is the lack of access context modeling. Access context can constraint specific conditions that must be met before the access. Finally, no explicit concept of organization and negative permission makes it inconvenient to grant permissions to a group of users except particular individuals from the group (Liang Xiao 2007).

### 2.3.7 Information Governance in NHS's NPfIT: A Case for Policy Specification

Becker in (Becker 2006) discuss about the specification language called Cassandra which used in implementing United Kingdom (UK)'s National Health Service (NHS) National Program for Information Technology (NPfIT) which also known as Spine. The characteristic of Spine are:

- Spine will be extremely large, holding life-long EHRs of 50 million patients.
- The system is widely distributed: user of the system have the interaction with ten thousands of local clinical information systems.
- The rules governing access to patient information which must be adhered by the user of the system. The rules include global and local policies.
- The state of the system, policies and user of the system are prone to change. Such changes must be implemented quickly to prevent future interruptions.
- There are many issues arose in term of misunderstanding.

This paper suggests adoption of the trust management approach which has been introduced by Blaze at al in 1996. Blaze et al describe access authorization based on digitally signed credentials containing principals' attributes rather than mere name bindings, thereby enabling mutual strangers to share resources in large distributed system. This paper suggests the use of employing policy specification in the development of any nation-wide EHR services. This paper demonstrates the information governance rules using Cassandra, a formal specification language.

### 2.3.8 An Adaptive Security Model for Multi-Agent Systems and Application to a Clinical Trials Environment

Xiao and friends in (Liang Xiao 2007) describes the use of security policy rule scheme to express security requirements in relation to affective roles. This technique used to overcome the weaknesses of Role Based Access Control (RBAC). Complex considerations are related with the management of different levels of access rights to multiple types of resources by users distributed among and managed by multiple organizations. These organizations need to use resources from others and also need to prevent their own resources from unauthorized use. On one hand, if a system is over restrictive in resource access control then the system cannot be fully use of. On the other hand, if a system is not sufficiently restrictive then the organization's private data is in danger of being exposed (Jaijit Bhattacharya 2006; Liang Xiao 2007). These constraint entail flexible security policy management and organization need to be able to configure policies themselves to reflect their actual changing needs. We need an adaptive security model that is configurable and reusable across application.

In 1988, (Miro semantics for security) (ALLAN HEYDON 1990), theys implemented and designed a visual language for specifying properties of large software systems. The visual notation has been applied to the security class. The Miro constructed from boxes and arrows that could be changed depending on the class of properties. The boxes represent the individual processes and files or collections of processes and files, while the arrows represent the rights. The fundamental, as cited, is simple: access rights matrix, where the processes and files have a set of rights that govern the access. Miro has the ability to express constrains on the relationships within boxes and between them called cables, constrains are a part of type information of a box. Miro solves many problems, however, applying it to other domains not yet been approved. The possibility of using visual approach to giving semantic instead of the standard denotation approach has not been explored yet.

Guy Edjlali, Anurag Acharya, and Vipin Chaudari (Guy Edjlali 1998) have presented a history-based access control mechanism that is aim to a selective history of the access request made by a program, thereafter use this history for the purpose of improving the

differentiation between safe and potentially dangerous requests. As mentioned, the mechanism has the potential to expand a set of programs without compromise the security or the ease of use. History-based access-control stated as a suitable mechanism for mediating accesses from mobile code. Identity of program, efficient maintenance of request-histories, persistence of policies and histories, grouping privileges, and composition and fail safe defaults, are the history-based access-control issues. The Deeds access-control policy consists of data structures for maintaining event-histories, handlers for the mediated events, and the auxiliary variables to facilitate the management of multiple policies. Once the security event occurs, control is transferred to the Deeds security manager to determine the class-loader, subsequently, the Deeds security manager invokes the event manager which maintains the set of handlers in the order they were attached to the event. Deeds has been approved comparing wit many other techniques, however, the performance of event dispatching seems has not been approved.

David Harel wrote a paper entitled "On Visual Formalisms" (Harel May 1988) that explaining about the higraph. Higraph can be assume as graphical language as it use graph to visualize formalism. In this paper, he describes how higraph representing the entity relationship diagrams, semantic and associative network, and dataflow diagrams. Harel stated higraph can represent the nature of variety of computer related system and situation. Harel believes that in future higraph offers assistance for daily technical and scientific chores.

Butler W. Lampson wrote in (Lampson 1974) describing the motivation of protecting computer system in the first place. He then explains about the process of protection between domains that are sharing and exchanging data or information. He proposes the use of identifier name for both domains who wish to interact. Besides that, he also suggests a systematic way to determine what kind of information to be shared as well as the control process of sharing within the environment (processors). He introduces the access matrices where domain can have access to the object depending on the access matrix. This paper also presents some implementation techniques. In my opinion, this paper has no information regarding the security language but it might be useful in terms of the protection techniques.

Authorization Specification Language (ASL) (Jajodia 4-7 May 1997 ) is a logical language that designed to support various access control policies. The policies include derivation of authorizations, conflict resolution, access control, and integrity constraint checking. In the paper, they listed two constraints of ASL. A. Extend the model to the consideration of administrative policies regulating the insertion of different rules by the user and B. how the model can be applied in the representation and enforcement if complex organization's security policies. Adding to that, we found ASL is not so complete to cover various policies in HIS security. It is hope that this study will be overcoming the second limitation of ASL as mentioned. Further discussions about ASL will be in Chapter 4.

LaSCO (Hoagland July 1998) is a graphical approach for specifying security constraints on objects, in which a policy consists of two parts: the domain (assumption about the system) and the requirement (what is allowed assuming the domain is satisfied). Policies defined in LaSCO have the appearance of conditional access control statements. The scope of this approach is very limited to satisfy the requirements of security management (Nicodemos Damianou 2001). LaSCO is a formal policy language based on graphs. Using LaSCO, one can specify constraints policies which constraints the use of resources on a system under given circumstances. LaSCO also specify policies in an object-oriented program. The system to which the policy is applied consists of series of events, occurring between a pair of objects.

As cited in (Carlos Ribeiro 2001) SPL: An access control language for security policies with complex constraints been referred. This paper generally discussed about a security policy language that allows organization to express and keep their global security policies in single description. This language proposed the concepts of permission and prohibition, and some restricted forms of obligation. They noted that this paper is a first step towards a security framework, which also includes the specification and enforcement of authentication policies, tools to verify the consistency of both specifications with other systems in the organization. Luckily, they have their tool that verifies the cross consistency of an authorization policies described in SPL and a workflow specification.

Ponder (Nicodemos Damianou 15 July 2002; Nicodemos Damianou 2001) is the most popular security language used in these distributed system era. Ponder is an object

oriented language for specifying security and management policy for distributed object system.

These two units summarized the literature reviews conducted to identify the steps to create a formal specification language. These literatures happened to be assistance for us to conduct a correct or at least an appropriate way to create the security language for distributed system.

## 2.4 Formal Specification Languages

Formal specification language is a general language created to allow one to develop and analyze precise models of computing systems, based on an internationally standardized notation. Formal language is used in the early stages of development; such a model can serve as a system specification, as an aid in checking the consistency and completeness of user requirements, as a blueprint for system design or coding (Kainhofer 2000). As in (Lamsweerde 2000) formal specification is the expression in some formal language and at some level of abstraction, of a collection of properties some system should satisfy. A specification also must satisfy some higher-level specification and be satisfied by some lower-level specifications. The stated 'formal' is not 'precise'. A specification is 'formal' if it is expressed in a language made of three components; rules for determining the grammatical well-formedness of sentences (the syntax); rules for interpreting sentences in a precise, meaningful way within the domain considered (the semantics); and rules for inferring useful information from the specification (the proof theory).Other than formal language, in market we have UML which have the same purpose but the difference is UML in diagram based. There are many types of formal languages in market and each of them has its own specialty. For this research purpose, we looked into two types of formal languages; VDM and Z Language.

### 2.4.1 VDM– SL

VDM- SL stands for Vienna Development Method - Specification Language. Generally, this specification language is able to construct a number of different system operations. It used model oriented method which consists of mathematical object like sets, sequences and finite mapping. It also has ability to model informal requirement by restricting

specified data types called data invariants. VDM-SL has the pre and post condition ability which can restrict what should be before and after the evaluation of system's operation. It also has the ability to validate the language using its own subset inside VDM-SL.
The weaknesses that makes this language not suitable for representing the security policy for HIS is it doesn't support the specification of dynamic systems (Kainhofer 2000).

### 2.4.2 Z Language

In (Spivey 1992) cited Z Language used for specifying information systems and developing rigorously checked design. Z language is grounded in mathematics. In Z Language, it has two main parts; the first part is the declaration area. Here the entire domain related with the operation will be declared. After that it will have a set of rules that specify what must be fulfilled before the operation can be performed. It has special mathematical symbol describing what objects exist, and how relationship between it may be made into specification. Listing all the best things in Z Language, still, doesn't make it suitable to present the security policy health information system. In addition, HIS is now in need for dynamic language that able to adapt changes in organization and environment quickly with minimal updates and interruption of current system.
This chapter solely describing all the works and researches that have been performed that is related with this study. The literature review commence with examining the various existing security model which have been introduced by the masterpiece to overcome the security problem. Afterwards, we will be presenting several languages that have been used ever since 1988 until now. The languages are not solely security languages, there are various kind of languages initiated for many reasons and have quite relation with this study. For instance to visualize formalism and to represent the complexity of computer system. This chapter continues with brief discussion about formal specification language such as Z Language and VDM-SL. Then, it will present the example of security languages that have been used all these years. From these studies, hoped the readers will get clear picture the reason of not using the existing language which then brings to the idea of proposing DiHIS Security Language as the solution to the policy based management for HIS.

# CHAPTER THREE

# ISSUES

This chapter discusses the essential issues that involved and closely related with health information system. These issues are necessary and to be taken into consideration before commencing implementation the health information system in any country. Each indentified issue discussed to justify why each of them provides a significant affect to HIS implementation.

## 3.1 General Framework

Commencing health information system is not simple and it does not happen in one night. It requires well planning, proper team of execution with co-operation with the all involved organization within HIS. The crucial things to do before proceed to build the health care network; we need to identify the general framework in order to implement the HIS.

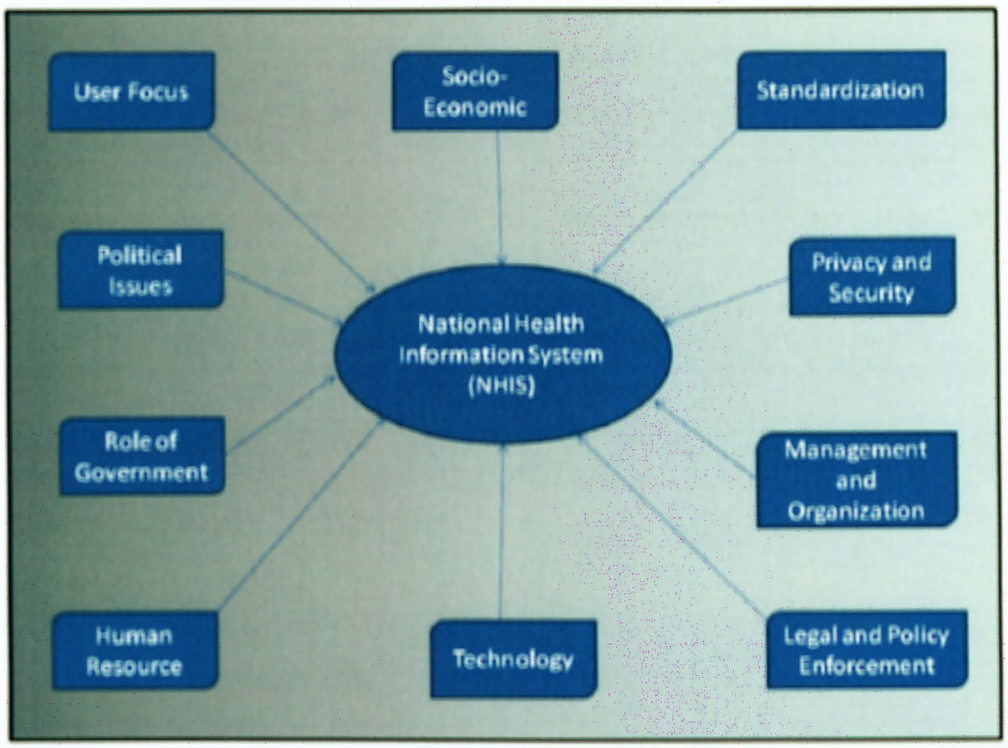


**Figure 1 General Framework for distributed HIS**

Figure 1 shows all ten areas that need to be tackled before distributed HIS can be implemented in any country. Each of them plays their own role that will largely determine the success on distributed HIS. As stated in (William W. Stead 2004), action is necessary at all levels, by federal and state government, regions and communities, and health care providers.

### 3.1.1 Role of Government

Government is the main donor for health information system projects. Money alone is likely to be insufficient unless accompanied by sustain support to the system development coupled with allocation of responsibilities(Carla AbouZahr 2005). Government should commence the HIS with capturing all the elements in the framework of distributed HIS. Useful research followed by well planning can lead to clear objectives and requirements. Then, HIS will be developing because we know what the needs are, what is unnecessary, what we do not have and what we have.

### 3.1.2 Legal and Policy Enforcement

**Legal Enforcement on Adoption of NHIS**

In the adoption of distributed HIS, it is important to gain support from the stakeholders within HIS. Without their support and collaboration, HIS cannot be a successful. Each of them has their own responsibilities which will be determined by the government and it is crucial to ensure that each organizations or stakeholders are following the right path towards implementing HIS in given timeframe.

**Privacy and Security Law Enforcement**

In the adoption of distributed HIS, it is important to gain support from patients because they are the focus user of the HIS. Without their trust, it's hard to get their agreement in sharing their personal health information throughout the system. In order to gain their support and trust, Malaysian government should have law regarding the security and privacy protecting their personal health information. Currently the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the broadest legislation addressing privacy and security of personal health information system. However, the HIPAA Privacy and Security Rules do not address specific privacy and security issues of a distributed HIS (Stokes 2005). HIPAA is widely used in United States of America. The purpose of law is to protect the patient's privacy and confidentiality as well as a reminder for others to always uphold the privacy concept otherwise punishment will be executed.

Besides law enforcement on security and privacy, one interviewee suggested establishment of an exceptional body that is responsible to carry out and uphold the security and privacy policies and laws through the time.

### 3.1.3 Privacy and Security

The patient expressed their concern about security and privacy repeatedly and has become a live issue in a number of countries. These issues must be understood clearly and distributed HIS must ensure that safeguards are adequate to protect data exchange and sharing.

*"The literature and anecdotes suggest that privacy and security present substantial challenges and even barriers for most developing or operational HIS"*. (Sheera Rosenfeld June 2007).

Further discussion about these issues is in Section 3.

### 3.1.4 Political Issue

Leaders, both within the national government as a whole, and within health ministry, need to show strong support for HIS, in order to overcome both external (donor) and internal (staff) resistance.

### 3.1.5 Management and Organizational

These issues related between the effectiveness of system implemented in the hospital with the hospital management.

> *"Past experience suggests that efforts to introduce clinical information systems into practice setting will result in failures and unanticipated consequences if their technical aspects are emphasized and their social and organizational factors are overlooked. ... Several decades of experience with computer-based information systems make it clear the critical issues in the implementation of these systems are social and organizational, not solely technical."* (Anderson 1997)

Therefore, the successful of HIS also depends on the support and will from the staff. This is important to make sure staff did not assume IT as a burden in their daily work. Risk assessment process can be helpful for the managers to undergo these issues specifically. On the same time, they can create an IT organizational environment in the hospitals which lead to successful HIS.

### 3.1.6 Human Resource

This issues focus on the availability of experienced staffs to manage the HIS. Currently our hospitals and clinics which have CIS or HIS, these systems developed by vendor (CERNER) originally from Kansas City, USA. And when the system implemented, the vendor will give some sort of training for the staff on using and maintaining the system. The problems that exist usually when errors in the system, the medical staff does not have

the knowledge to fix instead they have to call the maintenance to solve the problem. Sometimes the problem can be solved through the phone and sometime they have to wait for the responsible person to come directly to the hospital solve it. If the hospital has experienced staff, the waiting time can be reduced and problems can be fixed immediately. Hence, experienced staff is needed in order to manage the system to ensure every problem solved in the shortest possible time and reduce any delay clinical works.

### 3.1.7 Technology

Technology factors consist of hardware and software, the telecommunication infrastructure and other aspects that allow communication and sharing among healthcare institutions.

First, hardware and software availability to ensure the system will perform systematically. For instance, software applications and equipments especially in radiology, laboratory, intensive care and operation theaters where the system is interfaced directly into the equipment and whatever data or image produced will go directly online into the system.

The telecommunication infrastructures must able to support communication and information sharing among healthcare institutions. This lead to adoption of Local Area Network, Wide Area Network, Video-Conferencing, Satellite and Wireless application. But of course, the security aspects must be covered to ensure the confidentiality is not breached. The maintenance aspect must take into account to support these technologies with the intention HIS can be a successful.

### 3.1.8 Socio-Economic

HIS must consider this factor since patient comes from different background of education, different level of social ranking as well as different level of income. Each of them has different expectations. For patients with higher income, they can afford to go the private hospital where better service provided since the number of patient is not as much as in public hospitals. HIS must able to provide equal health service and treatment to everyone.

### 3.1.9 User Focus

Beside human resource aspects which focus on the staff, user (patient) focus is important since they are the main user of the system. Considerations need to be made since user comes from different races and different languages, different group of ages and different background of educations. They need to be educating accordingly about how their personal health information will be used inside HIS so that they will have better understanding. Without user understanding, there would be a problem gaining their trust and this can delay the adopting of HIS.

### 3.1.10 Standardization

The use of technology intended to allow communication and sharing applied within HIS. Currently, HIS in one hospital "cannot talk" with HIS in other hospitals. Without widely adopted standards and guidelines, interoperability and interconnection are not possible and the great potential of NHIS will be difficult to achieve (May 2003).

Technical standardization must be carefully and clearly set to ensure the ease of implementing NHIS. First, HIS platform should have the standards for the type of platform to be used is processor/ minimum speed, memory requirements, interfaces and peripherals. Second, clinical devices should have the standards for all the clinical devices to be interfaced or integrated with the HIS, including performance specifications, imaging devices, and their safety requirements. Third, video conferencing should have the standards such as date rate, picture resolution, frame rate type of camera, audio quality etc. Lastly, standard for various hardware used for interfacing the HIS with the communication network, including all types of terrestrial and satellite based network.

> *"In addition to technical standards, clinical protocols and guidelines are needed. Clinical protocols for HIS practice include preliminary scheduling process, and actual consult procedures. There is the need to evolve standards and guidelines to facilitate growth of practice of NHIS that is uniform and scientific."*(May 2003)

### 3.2 Proposed Database Connection within distributed HIS

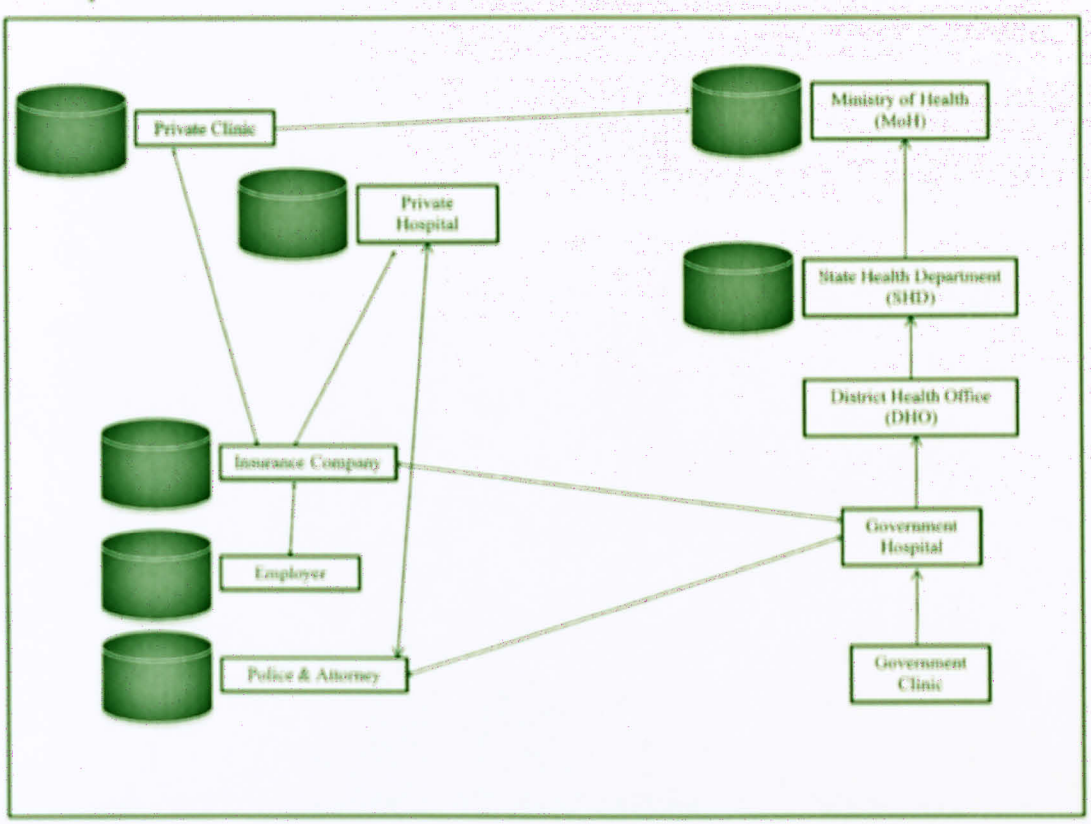


**Figure 2 Current Health Connection**

Figure 2 shows the current health connection in Malaysia. The arrow shows the flows of information reside in each organization to another health care provider/ organization. This diagram look simple but the real complicated connection when there are a number of government clinics, government hospitals, private hospitals, private clinics, insurance company and so on. Each database in the diagram belongs to the health care provider or organization beside it. This also means that they are practicing different kind of system and different database. This heterogeneity complicated the security planning and implementation. In order to have a safe sharing within distributed HIS, systematic and secure database connection among these health care provider or organizations is needed.

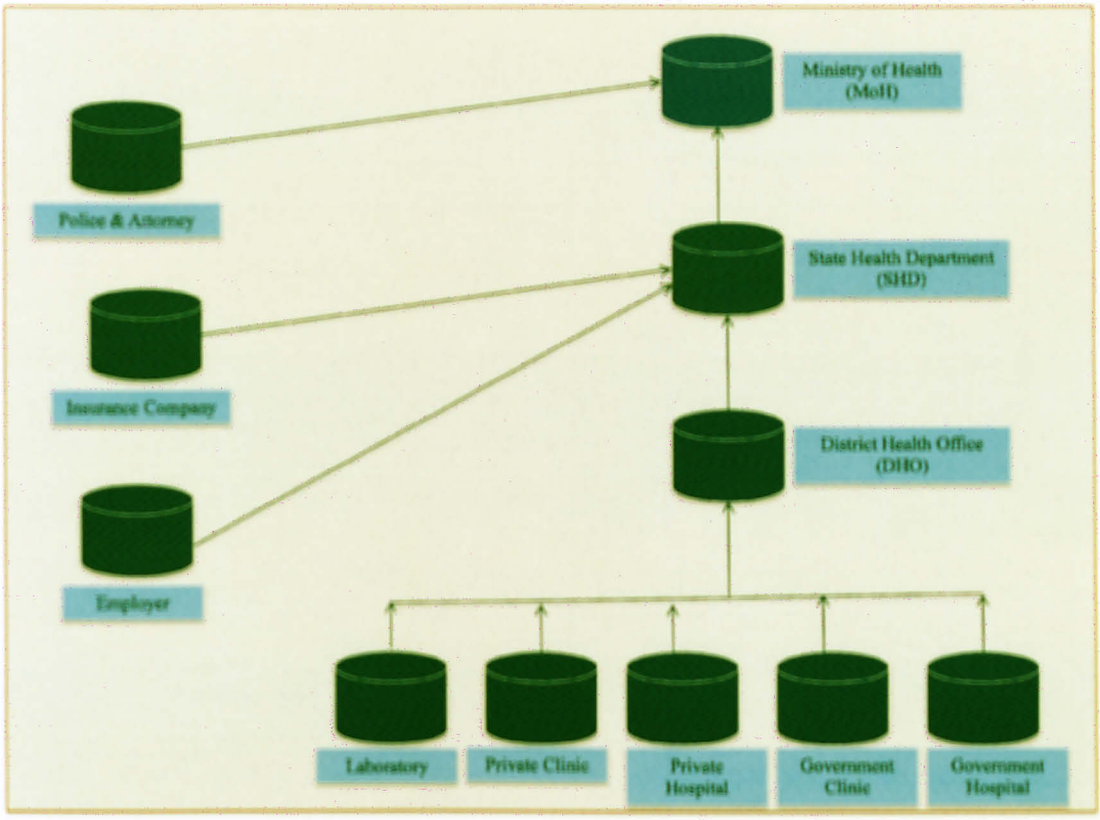


**Figure 3 Proposed Database Connection within HIS**

Figure 3 above is the proposed database connection which will provide ease of sharing as well as the standardize security planning and implementation.

### 3.3 Issues

From the interview conducted, they expressed their concern about the privacy and security issue. Even though computer-based electronic records can in many ways be more secure than paper-based records, the same technology raises trepidation about their privacy because of its capabilities of being copied, stored and disseminated by means of computers quickly when compared to paper based information records (Chaminda Jul 2004).

#### 3.3.1 Government Clinics and Hospitals

At each state, most of patient health records kept inside these two health care providers. Every day, they are processing a large number of medical activities concurrently. Most of these hospitals are legacies hospital and their method of keeping the patient medical

record is paper-based. In paper based systems, since there is only a copy of the patient's record, the whole record or a part of it can be lost, stolen or damaged, and information can be added, removed or modified without an audit trail (Chaminda Jul 2004). Having distributed HIS will assist them faster decision making or ease of sharing information (For instance, asking for one particular blood type from other hospital's blood bank).

- Clinician have too many work may result to human error (For instance mistaken entering the medical information of one patient to another)
- Clinicians are too busy may result improper patient health records monitor (For instance unauthorized access may happen without clinician awareness).
- Most of the clinicians is medical expert, they would need extra training to understand and use the system when NHIS is implemented – incur high cost.
- Because they are very busy with medical work, they could be reluctant to learn new system (For instance they will assume NHIS as a burden).
- Need to assign proper security policy to responsible clinician and must have transfer authorization if one is not available (For instance in case of emergency)

### 3.3.2 Private Clinics and Hospitals

Currently, private hospital and clinic are independent. They only required submitting a monthly report to health ministry. We have to understand clearly one thing about private clinic and hospital, their main objective is doing business and medical comes after that. Their focus on communicate among them in the same group. Besides that, if they need to communicate with other hospital (For instance, government hospital), the method are using phone, fax machine, and manually printed health records.

- these health care provider may reluctant to share information as proposed by HIS since they concern about their services (For instance do not want to share their expertise)
- they could be reluctant because they do not want to expose their business information to their opponents (For instance cost of operations and cost of medicine)

### 3.3.3 Laboratory

Currently, there are government laboratory and private laboratory. We will need these lab to be able "to talk" within distributed HIS especially during epidemic.

- test result need to be submit to DHO as soon as possible (For instance each test for disease require a number of days to come out and no further delay can be afford in order to save lives

### 3.3.4 Ministry of Health (MoH)

Currently, Ministry of Health has connection with the government clinic and hospital only. The reports send by the lowest level (clinic and hospitals) to District Health Office (DHO). Each DHO will consolidate all the report received from these hospitals and send the report to the State Health Department (SHD). Each SHD will consolidate the reports and send it to the MoH. Moh will then receives all these report from each state as well as private clinics and hospitals to be consolidated.

With the proposed database connection within NHIS, private clinics and hospitals will be under each DHO. The burden for MoH to consolidate report directly from private clinics and hospitals will reduce. MoH will need to consolidate the report once received from each SHD.

One of the unit inside MoH is Dieseases Control Division Unit (DCD) require accurate and complete information in case of outbreak. (For instance the patient address, travel history, the hospital patient is being treated, and the physician's name).

- Situation stated above must happen in fast, accurate and secure process in order for DCD staff to able prevent the outbreak from spreading.
- Ease of monitoring the outbreak within NHIS and better decision making (For instance, traditional way is using phone)

With the proposed database connection within NHIS, organizations such as Insurance Company, Employer and Police and Attorney will have to request information from MoH.

- the purpose is for MoH to able control the flow of information accessed by these organizations.

- An agreement or memorandum of understanding must be agreed by all parties about what information allowed for sharing, who is allowed, and how the process will be executed. (Fill in form or grant access)
- Using this way, the patient's privacy will be kept and only the needed information is being used in sharing process.

The information exchanged and the services provided are sensitive in the sense of personal privacy of patient or staff involved as well as confidentiality of business information (Blobel 2001).

**3.4 Principles**

"There are four key questions that NHIS must address: (1) Who will have access to patient information? (2) Which information will be accessible? (3) What are acceptable purposes of information exchange? and (4) under what circumstances should users be able to access information?." (C. Abuo Zahr Aug 2005)

*Who will have access to patient information?* – The answer for the first question is available when we look at who is the person, entities, or organizations which using the patient health record. They are the patient themselves, Ministry of Health (MoH), insurance company, employer, physicians, nurses, pharmacies, health researchers, clinics, laboratories, police and attorney and person with bad intention also would want to access personal health record. In case of emergencies, the paramedics would need to access the patient records also.

*Which information will be accessible?* – Demographic data, medical history, admission and discharge information, appointment date, doctor's note, billing, material, lab result (blood test, X-ray), medicine and quantity taken, surgery performed (doctor in charge, cost) are some of the information kept inside the patient health record (Sheera Rosenfeld June 2007) Each entity describe before they have different attention to different data. It is important to discuss and defined the entity accessibility.

In a distributed and extended environment, it would be difficult to assign authorization and access right within extended domain to any principal specifically; principals are

grouped according to the role group. The grouping is assign based on their attributes or characteristic (qualification and skills). There could be based on profession, legally defined and regulation or policy defined (Blobel 2002).

*What are acceptable purposes of information exchange?* – The author in (Liang Xiao 2007) stated there's need for flexible security policy management and organization to ensure their changing need is fulfilled overtime. If one organization impose a very strict in access control, the resources or information might not be useful. On the other hand, if the organization is not sufficiently restrictive, then the data is in danger of unauthorized user.

Each entity has interest at different part of patient health records. For instance; health researchers would need detailed information about the disease such as age, diagnosis, and medical history for research purpose only. Hence, the name of the patient can be exception from the research. Instead of real name, they can assign special ID to the patient record (Liang Xiao 2007; Muhammad Sher 2007).

*Under what circumstances should users be able to access information?*

Answering the fourth question refer to the policy specify by the organization. The policy will define how security measures will protect the privacy.

### 3.4.1 Access Control

In computer security, discretionary access control (DAC) is a kind of access control defines by the Trusted Computer System Evaluation as "a means of restricting access to objects based on the identity of subjects or group to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control)".

In computer security, mandatory access control (MAC) refers to a type of access control by which the operating system constraints the ability of a subject or initiator to access or generally perform some sort of operation on an object or target. In practice, a subject usually a process or thread; objects are constructs such as files, directories, shared

memory segments, and etc. Subjects and objects each have a set of security attributes. Whenever a subject attempts to access and object, an authorization rule enforced by the operating system kernel examines these security attributes and decides whether the access can take place. Any operation by any subject on any object will be tested against the set of authorization rules (policy) to determine if the operation is allowed.

With mandatory access control (MAC), this security policy is centrally controlled by a security policy administrator; users do not have the ability to override policy and, for example, grant access to files that would be otherwise be restricted. By contrast, discretionary access control (DAC), which also governs the ability of subjects to access objects, allows users the ability to make policy decisions and or assign security attributes. MAC- enabled systems allow policy administrators to implement organization-wide security policies. Unlike with DAC, users cannot override or modify this policy, either accidentally or intentionally. This allows security administrators to define a central policy that is guaranteed (in principle) to be enforced for all users.

This person must be an authorized and has provided necessary identification before allowed to proceed with the appointed tasks. Within HIS, assigning authorization is very complex. Through the use of ASL (Jajodia 4-7 May 1997 ), is not sufficient to grant access with subject and object for HIS background since it involved large number of staff. Moreover, it will take a lot of time to set the access control individually where most of them share the similar tasks. Having said that, Role Based Access Control (RBAC) (Liang Xiao 2007) been introduced which suggest access control to be given in a role basis rather than individually for distributed system. For instance, role nurses have their own tasks and doctors will have their own tasks. People to be grant accessed by pointed at the group he/ she belongs to. But the problem did not stop there. The problem rise in the case where nurses in one hospital has different ability tasks performed from nurses in other hospitals (Liang Xiao 2007). From the situation above, we can assume that with introduction new technology, it generates new problems that need to be solved urgently.

### 3.4.2 Minimum Access Entitlement

User is entitled to a minimum access (For instance, limited to reading and/r viewing only). Authorization is required to enable user to create, save, update and change or

delete specific information. Access entitlement is periodically reviewed taking into account the user's roles and responsibilities (scope of work). (August 2007) Minimum access entitlement is deeply encouraged to limit the number of people accessing a large data. Having too many people accessing the same and large data would risk the data in term of privacy. If too many people can access the critical data, then it wouldn't consider a secret already.

### 3.4.3 Accountability

All users are accountable for their actions with regard to the organization's assets.(August 2007) This is very crucial since human are prone to error. Each person who are accessing to the system or using the system must have the identification code that unique to himself, even though in some distribute system, they practice domain group concept. For instance, if a doctor has given a wrong medical prescription to his patient, he cannot deny his action. Because with the adoption of this NHIS, each result of test, meeting, diagnosis are entered into the system. All the information inside the system acts as proof of action that has been performed by each domain-group.

### 3.4.4 Segregation

The task to create, delete, update, change and validate data must be segregated to avoid unauthorized access to protect the organization's assets from errors, classified information leakages or manipulation. The segregation also encompasses actions taken to separate operational groups from the network.(August 2007) In explaining this situation further, consider this situation. If a doctor A is purposely want to harm his patient, he would give the wrong medical prescription to that patient and he can entered a different prescription inside the system. In this case, the doctor can blame the pharmacies wrongly gave medical prescription to the patient. If we have segregated the task and action, it's easier for the pharmacies to defend herself by showing the prescription notes given by the doctor A.

### 3.4.5 Auditing

Audit is an action undertaken to identify incidents regarding security or to identify issues which threaten security. It involves preservation of all records pertaining to ICT's security action (For instance, computers, servers, routers, firewall and network must be programmed to generate and save the security logs or audit trails). (August 2007)

### 3.4.6 Compliance

The security policy must be read, understood and adhere to in order to avoid any breach will may compromise ICT's security. (August 2007) This concept can only be achieved if each people involved inside NHIS have the sense of responsibility. They must feel that protecting one's privacy is as important as they are protecting their own.

### 3.4.7 Recovery

System recovery is essential to ensure availability and accessibility. The main objective is to minimize interruptions or loss due to being unprepared. Recovery can be undertaken using backups and by establishing a plan for disaster recovery. (August 2007) This situation is common for all information system and there are many types of companies offer their product for recovery of data.

### 3.4.8 Interdependence

The above principles complement and support each other. Hence, the steps taken to diversify the approach as much as possible when arranging and designing security mechanism are essential to ensure maximum level of security.(August 2007)

### 3.4.9 Need to know Policy

The term "need to know", when used by government and other organizations (particularly those related to the military or espionage), describes the restriction of data which is considered very sensitive.

Under need to know restrictions, even if one has all the necessary official approvals (such as a security clearance) to access certain information, one would not be given access to such information unless one has a specific need to know; that is, access to the information must be necessary for the conduct of one's official duties.

As with most security mechanisms, the aim is to make it difficult for unauthorized access to occur, without inconveniencing legitimate access. The principle also aims to discourage "browsing" of sensitive material by limiting access to the smallest possible number of people.

It has been alleged that need to know (like other security measures) can be misused by some personnel who wish to refuse others access to information they hold in an attempt to increase their personal power, or to prevent unwelcome review of their work.

The need to know principle is at odds with most purposes of intelligence and research. While one part of an institution may have knowledge of some data, the rest of this institution as well as other institutions remain ignorant. Since experience shows that data shows its most valuable information only when freely connected, the need to know is in fact putting a limit on information that intelligence agencies can gather (even if there are no limits to the amount of data).

# CHAPTER FOUR

# DiHIS - SECURITY SPECIFICATION LANGUAGE

In this chapter, the main focus is to describe the syntax and the semantic rules of DiHIS security specification language. Adding to that, readers will be reviewing the comparison of ASL (Jajodia 4-7 May 1997 ), LaSCO (Hoagland July 1998), Ponder (Nicodemos Damianou 15 July 2002; Nicodemos Damianou 2001) and DiHIS representing a security model proposed by Ross J. Anderson (Anderson Jan 1996; Anderson May 1996). Before coming to that, the content of first section will be the introduction of DiHIS model overview. In this section, the model is explained and set of notation that been used within the mathematical model is presented. The chapter went further with discussion about policies and how DiHIS represent them. Then, this chapter proceeds with comparison among DiHIS with three other security languages which are ASL, LaSCO, and Ponder. The result of comparison summarized in a table and discussed at the end of this chapter.

## 4.1 DiHIS model overview

DiHIS represents Distributed for Health Information System which it's a security specification language initiated focusing on policy based management within health care network. With the introduction of information technology (IT), our everyday life has been impacted by the application of IT almost everywhere. The great interest of sharing

information among entities separate by distance open a new road for network system initiated. With the emergence of health information system, they would aim for sharing information which leads to several benefits such cost cutting and saves lives.

Despite all this benefit, still the most concern by the people is the security of health system in protecting their privacy. This lead to several problems where one of them is the management faced when the network has become wider. It's hard and costly to manage a distributed and large number of systems. Nowadays, the best way managing distributed system is by implementing policy-based management. This thesis aim to aid in bringing up a suitable language to help industry implement the security policies in their organization effectively.

Below is the DiHIS diagram where this language suggests each organization within the health network to be grouped according to their importance at different levels. This system assumes each entity in each level as object and object should have a set of subject. There also a general policy that must be adhered by all object in this system and there also policy unique to the level only. The diagram below shows the DiHIS Diagram which provides an example of how to place the organization into different level.

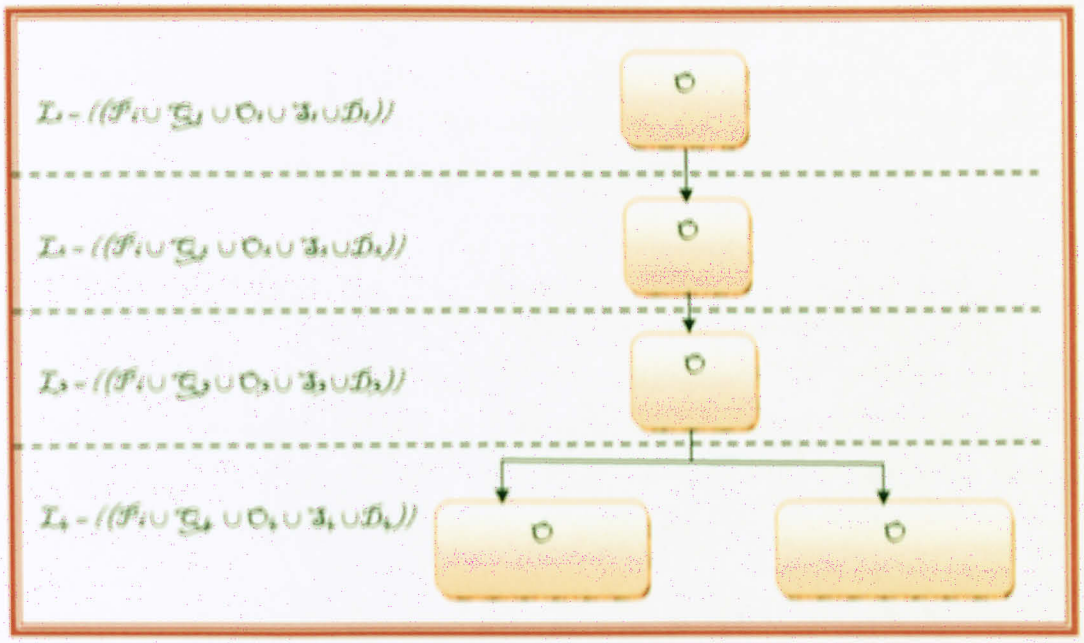


**Figure 4 DiHIS Diagram**

Figure 4 above describes overall of the model. Different object and subject were placed at different levels. The label $\mathcal{L}_i$ ; $\mathcal{L}$ denotes level while $i$ denotes a natural number and is greater than or equal to one and its infinity. The counting is in ascending order. DiHIS allocated the level number one to represent the highest level. As the level number increasing, it means the lower level they are. Each level will be appointed its own sub-policy (not shown in the diagram). Sub-policy is unique for each level. The sub-policy represented in the system as $\mathcal{G}$. The object represents the multi-organizations in the system. Object located in the system according to different level they belong. One object can be at one level only at one time. Sharing object between two different levels at the same time is not allowed since it will lead to conflict policy. The object in the system represent as $\mathcal{O}$. As for the subject, it represented as $\mathcal{S}$. Subject belong to the object. Each object will have a set of subject. In easier manner, subject's role is as department which belongs under its organization (In this example, the organization is the object). Not to forgetting, there also the general policy which stands the policy that is obligated to all object and subject in the system.

Once the objects (agent) have been placed in the level accordingly, it obligates to comply with the policy that incorporates in the respective level. A policy is a rule that defines a choice in the behavior of a system. Separating the policy from the implementation of a system permits the policy to be modified in order to dynamically change the strategy for managing the system and hence modify the behavior of a system, without changing its underlying implementation (Nicodemos Damianou 2001).

**4.2 Basic Definitions**

Distributed Health Information System (DiHIS) security language is created based on the Set Theory. The purpose of this language is to represent the policy which is usually in English language. This language dedicated for implementing security policies within distributed HIS. Below, the basic policies used in distributed system are discussed to give the readers an overview about DiHIS security language.

### 4.3 Access Control Policies

Access control policy is the policy that limits one's ability to perform task toward certain object or target (Damianou February 2002). There are a number of policies resides below the access control policies. There are authorization, obligation, refrain and other policies. Below is the first element of access control policies.

#### 4.3.1 Authorization Policy

Authorization policies define what activities an object can perform on the set of subject in the system. These are essential access control policies, to protect resources and services from unauthorized access (Nicodemos Damianou 2001). In distributed HIS, a number or person need an access to certain clinical record or data. Before a person (clinician or nurse) is authorized to get access to the patient record, he must be added to the set of E. E denoted Authorized Entity. E+ can be individual and also a group but every person must belong to a group. If one person who already added into the E but has not given any access, still he cannot perform any access to any target or object. E consists of several sets such as DOC (clinicians), NURSE, DOCR (referring clinicians), RESEARCH (researchers), and etc.

Clinical records always associate with patient. The set of clinical records is denoted as CR and the set of patient is denoted as PT. This relationship can be represented as a function f:CR→PT. The set CR has its own subset which logically, several different records created at different units even in one same hospital. The subset for each $CR_x$ represented as $CR_{x,y}$ where the symbol x denotes the unique ID of the clinical records belong to a patient x and y represents the different records. y represented using number for simpler differentiation among clinical records for each patient. $CR_{x,y} \equiv \{CR_{x,1}, CR_{x,2}, CR_{x,3}, \ldots CR_{x,u}\}$. For a simpler presentation for indication of this function, f:CR→PT denotes as X.

The term access can lead to a number of choices. It could be +OPEN, +APPEND, +CREATE, +READ, +DELETE, +VIEW, +ADD, and etc. This access can be only one of the choices and can also be all of it.

Within distributed HIS, allowing access restricted to several conditions or rules or constraints. There must be stated the type of file or record, the location of the file and the

< constraints D>

### 4.3.3 Refrain Policy

"Refrain policies define the actions that subjects must refrain from performing, in other words must not perform, on target objects even though they may actually be permitted to perform the action. Refrain policies act as restraints on the actions that subjects perform and are implemented by subjects". (Nicodemos Damianou 2001)

Eo ∈ E ∧ Eo ∈ [groups] | [groups] ⊂ E

↔ [access-]

X [target]

<Constraints>

<Constraints>

### 4.4 Transaction Policy

Transaction policy defines how the transaction process between each organization within HIS must be performed in order to ensure the security of the information transferred. The transaction can only be executed when two valid person or units recognized each other. There must be unit that request and the other received and process the request. In the first place, the requestor must send a set of request as well as its ID to the receiver. The receiver unit which denotes as Eer will then check the validity ID of the requestor which denotes as Eor before accepts the request for processing. After the receiver finished processes, it sends the result which represents as R' to the requestor. An acknowledgment of the result acceptance must be issues by the requestor units which denotes as Accept'.

During the transaction process occurs, both requestor and receiver are in the transaction zone. Transaction zone will only end when the receiver has received the acknowledgement of acceptance. A set of transaction represented as $\mathcal{T}_p = \{\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3, \ldots \mathcal{T}_j\}$. Each $\mathcal{T}_p$ contains several sets which are requestor ID, receiver ID, task, result, acceptance acknowledgement and time start (tv) and time end (tv+ tΔ).

EorID ∈ E+

$\mathcal{T}_{p\,(tv)}$ = (EorID, EerID, R)

$\mathcal{T}_{p\,(n+\,t\Delta)}$ = (EorID, EerID, R', Accept')

### 4.5 Obligation Policy

"Obligation policies specify the actions that must be performed by managers within the system when certain events occur and provide the ability to respond to changing circumstances. For example, security management policies specify what actions must be specified when security violation occur and who must execute those actions; what auditing and logging activities must be performed, when and by whom". (Nicodemos Damianou 2001)

This policy depending on event triggered. A set of event must be defined and represents as $EVENT_k$ = { $EVENT_1$, $EVENT_2$, $EVENT_3$,... $EVENT_n$} where k is natural number more or equal to one and its infinity. Each event has been assigned its actions. This process known as Oblig. The set of Oblig represent as $Oblig_r$ = {$Oblig_1$, $Oblig_2$, $Oblig_3$,...$Oblig_m$} where r is natural number more than or equal to 1 and its infinity. The relationship can be shown by a function f: EVENT ⟶ Oblig. For each $Oblig_r$ consist of several sets which are the sets of action (a), the executor (E+), the target or object (Eobj), time (t), and archive.

$Ev_{k=1}$

$Oblig_{r(k)}$ = (a, E+, Eobj, t, archive)

### 4.6 Need to Know Policy

The need to know is about giving the needed information at a specific time i.e emergency cases to the trusted requestor. The requestor will be getting access to what he is allowed only under need to know policy. In overcoming this problem, the system assume that there must be an agreement between the information provider with the requestor about what information are logically to be allowed for access during specified events. The system assumes that there will be a set of task or event that listed from the agreement. These tasks will be represented by a set $ts_n$={$ts_1$, $ts_2$, $ts_3$...$ts_k$} where ts is the task to be performed and n is a natural number which must be greater than or equal to 1 and until infinity. The requestor will enter the special task number or code into the system, the system will recognize the principle it carried and process the information as specified.

Then, the system will return the information or data needed to the requestor. This situation will comes with specified restriction such as limit the person who allowed to request and the size of the information and the period of need to know will last. The example of this situation can be read at Chapter 5.

### 4.7 Security Languages to Represent Security Policy Model in Clinical Information System

This section will be divided into four sub-sections where each section describes in detail one security language to represent the 9 principles of Security Policy Model in Clinical Information System. Below are some important definitions needed to be stated before we start using a language to represent security policies.

- Closed Policies (Positive Authorization): An access is granted if there is an authorization stating that the user can access the object.
- Open Policies (Negative Authorization): A user can access any object unless it has been explicitly denied.
- An Access Control Policy: is a set of rules defining what is authorized.
- An Access Control Mechanism: is a policy implementation to ensure that all accesses are in accordance with the underlying policy.

#### 4.7.1 The Authorization Specification Language (ASL)

The first language to represent the security model is ASL. ASL (Jajodia 1997) is a language for expressing the authorization according to access control policies. ASL supports a model based on two elements, an object (o) which could be a file or directory in an operating system or table in relational database, and an authorized entity who could be user (U), group (G) or roles (R). An authorization policy in ASL is a mapping that maps 4-tuples $(o,U,R,a)$ to the set {+, -}, where $o$ is an object, $u$ is a user, $R$ is a role and $a$ is an action, while + means authorized and – means denied.

ASL designed principally to express the following rules:

*Authorization Rules*: used by System Security Officer (SSO) to allow or deny accesses to objects explicitly in the following form:

*Cando (o,s, <sign>a)* ← *L1 &.....&Ln*

This predicate symbol states that a subject *s* can (*Positive authorization sign* = "+") or cannot (*negative authorization sign* = "-") perform the action *a* on the object *o* under the condition that are specified by *L1&...&Ln* where *L1...Ln* could be one of the following literals: in, dirin, or typeof. Principle 1 in the following section is an example of this rule.

*Derivation of rules*: used to derive implicit authorizations from explicit authorizations and determine the authorization policy. Indeed it is for expressing propagation of authorization along subject's hierarchies, In addition derivation rules can express some kinds of implication relationships such as the derivation of an authorization in the base of the presence or the absence of other authorizations. The derivation rule has the following form:

*Dercando(o,s,<sign>a)* ← *L1&...&Ln*

The right hand side of this rule derives a positive or negative authorization. (determined by *<sign>*) for a subject *s* to perform the action *a* on the object *o* according on another authorization in the right hand side *(L1&...&Ln)* where *L1...Ln* could be one of the literals: cando, dercando, done, do, in, dirin or typeof.

*Resolution Rules*: used to regulate how to resolve any conflict could accrue between authorizations specified by the authorization rules *cando* and *dercando* as in the following form:

*Do(o,s,<sign>a)* ←*L1&...&Ln*

This form states the enforcement of exercising (if *sign* = "+") or forbidding (if *sign* = "-") an access on an object by a subject s in case of a conflict in the Authorization Rules (*cando or dercanco*) in the right hand side.

*Access Control Rules*: to be used to regulate access control decisions on the basis of authorization specified by the authorization rules. Access control rules have the following form:

*Grant (o,u,R,<sign>a) L1&...&Ln*

This form states that a request submitted by a user u with active roles R to perform the action a will be allowed (sign ="+" or forbidden (sign + "-") based on an authorization condition on the right hand side L1&...&Ln is either cando, dercando, done, do, in, dirin, or typeof.

*Integrity Rules*: used to express different kind of constrains on the specifications and the use of authorizations. Integrity rule is a rule of the form:

*Error()* ← *L1&…&Ln*

Where *L1&…&Ln* is either cando, dercando, done, do, in, dirin, or typeof. This rule derives an error every time the conditions in the right hand side of the rules are satisfied.

Principle 1:

A subject s can read from and write on a clinical record *clinical_record* if only she is in the access control list *Clinical_Record_ACL* (here specified as a role) of that record. The following is just an authorization rule. The left hand side part *(cando(clinical_record,s +read/write))* is the authorization that is to be given and the right hand side part *(in(s, Clinical_Record_ACL))* specifying conditions that must be verified for the authorization to be hold.

← *cando(clinical_record,s +read/write)*

← *in(s, Clinical_Record_ACL)*

Principle 3 and 4:

The following code states that a subject patient must read his access control list *Clinical_Record_ACL* if it has been appended by a subject *clinician* who is authorized to do so.

← *cando(Clinical_Record_ACL, clinician, +append).*

*do(Clinical_Record_ACL, patient,+read)*

← *cando(Clinical_Record_ACL, patient, +read).*

← *done(Clinical_Record_ACL, clinician, append).*

← *cando(Clinical_Record_ACL, clinician, +append).*

Observations:

We can see clearly that ASL can represent Principle 1, 3 and 4 only. The limitation or weaknesses of ASL is that this security language can only express the authorization in two ways; allow and deny. For example in Principle 6 stated, an audit operation must be performed after authorized access is done. ASL failed to represent any consequences

action that must be done after one access is done. Another limitation of ASL is unable to control the number or access to certain records. The need of aggregation control is stated clearly in Principle 8. Thus, this language is unable to represent the other six principles of Security Policy Model in Clinical Information System.

### 4.7.2 A Language for Security Constraints on Objects (LaSCO)

The next existing security language which we used to represent the 9 Principles is LaSCO. LaSCO (Hoagland July 1998) is based on a model where a system consists of objects and events. The attributes on an event denote the specifics of the event's executions. Policies in LaSCO are stated as policy graphs which describe a specific state of the system (domain) and specific access constraints (requirement). Predicates are annotations near the nodes (objects) and the edges (event) to describe the domain (in the graph written as bold text, i.e. **type = "user" and method = "access"** -- as in Figure 5 --) and requirements (in the graph written as normal text). LaSCO uses variable called *policy variables*. A policy variable represents a value of an attribute and relates attribute values associated with different objects and events. Variables may appear as operands in domain (i.e. in Figure 5 **ID=$UID**) and requirement predicate (i.e in Figure 5 $UID ∈ ACL). They are denoted by a "$" prefix.

Principle 1:

The policy graph in Figure 5 indicates that a user/subject needs to have his/her/it ID that represented by the policy variable $UID included in ($UID ∈ ACL) the access control list of the clinical record in order to have an access to it.

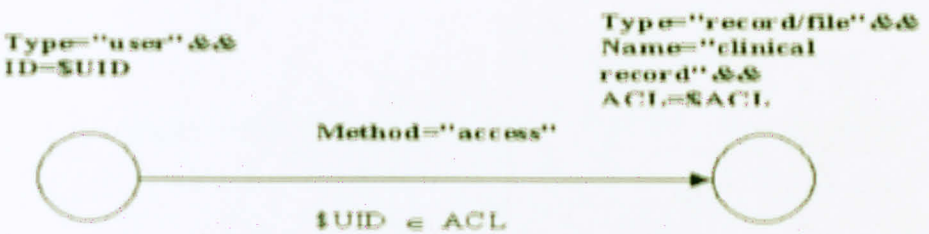


**Figure 5 A security policy graph represents Principle 1 of the clinical security policy**

Principle 2:

If the user's security level/ clearance (represented by the policy variable $UL) is not the same as (stated by the event requirement $UL ≠ $FL) the clinical record's security level (represented by another policy variable $FL) a clinician may create a new clinical record with new access control list as shown in Figure 6.


**Figure 6 A security policy graph represents Principle 2 of the clinical security policy**

Principle 3:

The policy graph in Figure 7 states that a user (represented as an object, which is stated by a set of attributes *type* and *position* in addition to policy variable *$ID*) can only append (represented in the policy graph as an event called method with value "append") the access control list for a clinical record (represented as an object, which is stated by a set of attributes *type* and *name*) if she is marked as responsible clinician (this condition represented as a requirement says that the ID of that user has to be the value of attribute called *responsible_clinician*).

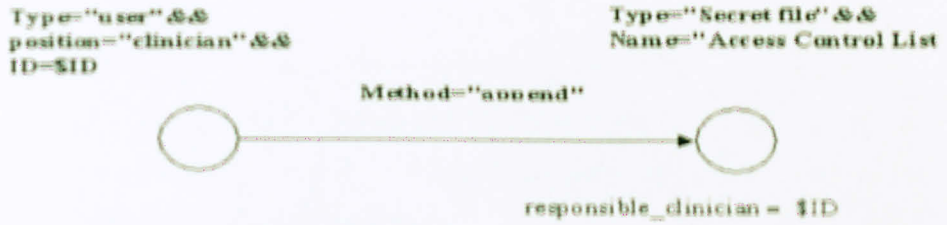


**Figure 7 A security policy graph represents Principle 3 of the clinical security policy**

Principle 4:

Since Principle 4 includes two events under different restrictions, we will divide it into two principles: Principle 4a considers the part that says the responsible clinicians must

notify the patient of the names on his record's access control list when it is opened, of all subsequent additions, and principle 4b considers the part that says whenever responsibility is transferred the patient's consent must also be obtained, except in emergency or in the case of statutory exemptions.

Principle 4a:

The policy graph in the Figure 8 specifies the first part of Principle 4 by restricting the method *add* to be executed after the method *message* (where *add* and *message* are events and the restriction ensured by a security requirement that enforces the order of these two events *Time>$ST*). So adding a new user to the access control list will not be allowed before sending message to the patient containing the name of the user who it is proposed to be added to the access control lost of his clinical record.

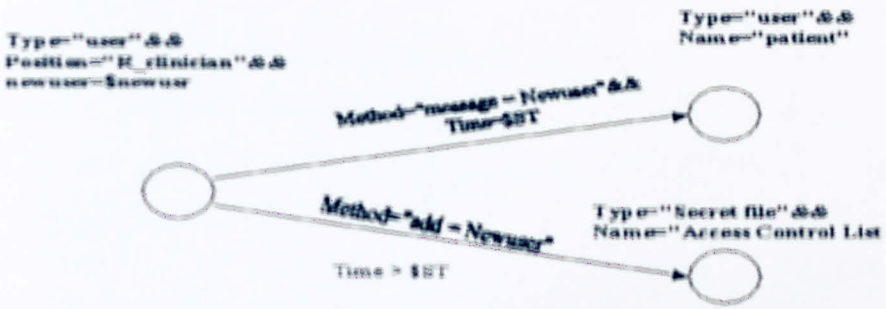


**Figure 8 A security policy graph represents the first part of Principle 4 of the clinical security policy**

Principle 4b:

The policy graph in Figure 9 specifies the second part of principle 4 as following: the event change responsibility is restricted by either the case in an emergency or the other event *Name="Consent" && Permit=$PM* has been performed and the consent has been given *$PM=true || Case="Emergency"*.

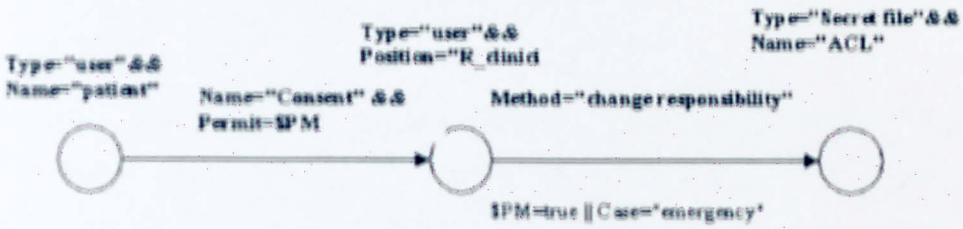


**Figure 9 A security policy graph represents the second part of principle 4 of the clinical security policy**

Principle 5:

The policy graph that is shown in Figure 10 states that event *delete* can be called by a *subject* to delete a *clinical record* (an object) if and only if the system date *$sysdate* (policy variable) is greater than or equal to the expired date of that clinical record *$Edate* (policy variable).

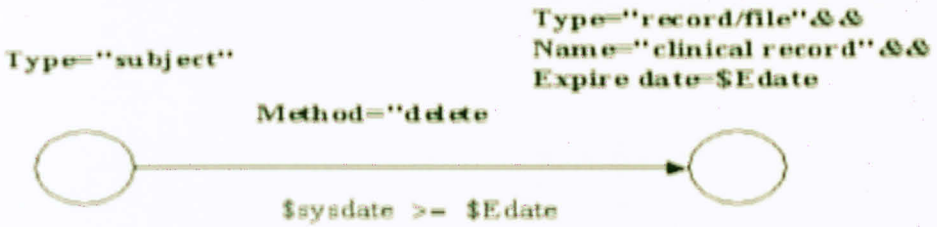


**Figure 10 A security policy graph represents Principle 5 of the clinical security policy**

Principle 6:

The policy graph that is shown in Figure 11 specifies Principle 6 by enforcing that a log record to be created contains a subject id *($SID)*, the access date and time *($SDT)*, the access id *($ADID)*, and the accessed clinical record *($RID)* for any access to the clinical record instance.

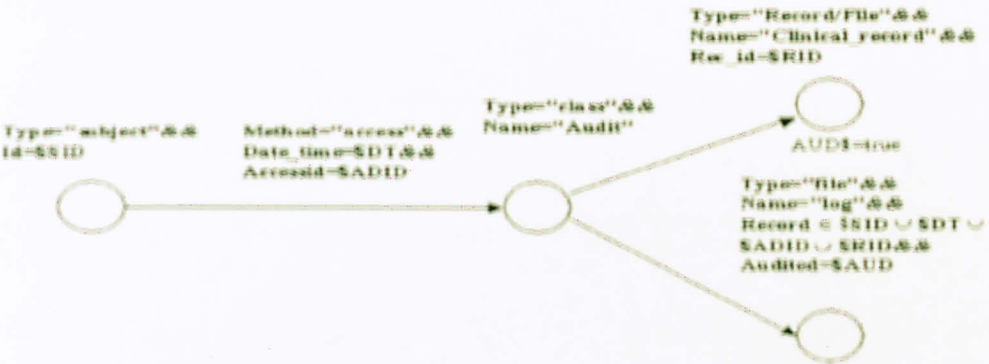


**Figure 11 A security policy graph represents Principle 6 of the clinical security policy**

Principle 7:

The policy graph that is shown in Figure 12 represents the information flow control by ensuring that the access control list for the source record is a subset of the access control list of the destination record *($ACL_B ⊂ $ACL_A)*

Note that: This principle is also implicitly shown in Principle 1 representation.

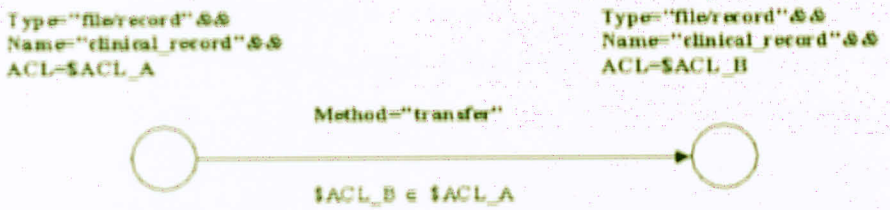


**Figure 12 A security policy graph represents Principle 7 of the clinical security policy**

Principle 8:

The policy graph that is shown in Figure 13 states that adding a new user to the access control list of a patient's medical record is not allowed before sending a message to the patients informing them that the user who is proposed to be added to their access control list already has access to personal health information on a large number of people *NoA>n* (where *NoA* is the number of accesses for the proposed user and *n* is a constant). Note that the order of the two events is enforced by ensure that the time of the add method is greater than the time of message method *Time>$ST*.


**Figure 13 A security policy graph represents Principle 7 of the clinical security policy**

### 4.7.3 A Language for specifying Security and Management Policies for Distributed System (Ponder).

Ponder is the third existing security language that used to represent the 9 Principles of Security Policy Model in Clinical Information System. Ponder is (Nicodemos Damianou 15 July 2002) a declarative and object-oriented language that includes constructs for specifying the following basic policy types:

- Authorization policies specify what activities a subject is permitted or forbidden to do. In other word specifying positive (**auth+**) and negative

**(auth-)** authorization policies (Principle 1 in the following section is represented as a positive authorization while Principle 5 is an example of the negative authorization).

- Obligation policies specify what activities a subject must do. These policies are triggered by events and are usually interpreted by a manager agent. An example of this type is found in Principle 2.
- Refrain policies define actions that subjects must refrain from performing.
- Delegation policies define what authorizations can be delegated and to whom.
- Composed policies are used to define a syntactic scope for specifying a set of related policies. There are four types of composed policies; groups, roles, relationships and structure management.
- Meta policies specify a permitted value for a valid policy.

The reader will note in the following section that all Anderson's principle fall into two types of security policies; authorization policies and obligation policies because these principles attempt to restrict the access control and/or enforce consequence actions.

Principle 1:

A subject *s* of type *user* is authorized (can perform the action) to read and/or append the clinical record *r* if and only if *s* is in the access control list of the clinical record *r.ACL* where *r.ACL* is the access control of the clinical record *r*.

Note that **type** is a type definition introducing a new user-defined policy type, from which one or more policy instances of that type can be created, **auth+** is a reversed word indicating that the following is a positive authorization policy, *principle1* the name of the policy type, **subject**<user> *s* means that *s* is a subject of the type *user*, **target**<clinicalRecord>*r* means that *r* is the **target** object of the type *clinical Record* to be accessed by the subject *s*, **action** is a reserved word followed by the action (*read and append)* that is needed to be authorized, and *belongs* is a user define function to check whether the subject *s* is a member of the access control list of the record *r* if so the positive authorisation will be allowed **result** = enabled;

**Type**

**auth+**principle1 (**subject** <user> s,

```
                    target <clinicalRecord>r,)
{
action read, append if belongs (s,r.ACL0
        {
result = enable;
        }
}
```

Principle 2:

In case of new clinical information for a patient *NewInformation* appears to be in a different security level *isDifferentSeecLevel*. With the exist access control list *currClinicalRecordAcl* a new access control list *newClinicalRecordAcl* has to be created.

Note that **on** is a reserved word followed by the obligation condition, and *isDifferentSecLevel* is a user define function to compare the new information againts the current security level and check whether it is a different security level in this case the mandatory action has to be performed **do** createNewACL(*newClinicalRecordAcl*).

```
type
        oblig principle2 (subject <responsible_clinician> s,
                          target <ACL>currClinicalRecordAcl,
                          newClinicalRecordAcl
                          <ClinicalData>newInformation)
{
on isDifferentSecLevel (currClinicalRecordAcl,
    NewInformation);
do createNewACL(newClinicalRecordAcl);
}
```

Principle 3:

A subject *s* of type clinician is authorized (can perform the alter/append) to alter and/or append the access control list of a clinical record *clinicalRecordAcl* if and only if *s* is marked as a responsible user in the access control list.

**type**

**auth+**principle3 (**subject** <clinician> s,

**target** <ACL> clinicalRecordAcl,)

{

**action** alter, append

if position (s, clinicalRecordAcl) = "responsible"

{

**result** = enable;

} }

Principle 4:

This principle is divided into two parts; the first principle 4a concerns informing the patient about any new addition to his clinical record access control list via the responsible clinician. This part is presented as follows: in case of adding new record *addNew* to a patient's access control list of his clinical record *clinicalRecordAcl,* consequently that patient has to be informed *informedPatient.*

**type**

**oblig** principle4a (**subject** <responsible_clinician> s,

**target** <ACL>ClinicalRecordAcl,

clinician newName)

{

**on** addNew(newName,ClinicalRecordAcl);

**do** informPatient (newName);

}

The second part of this principle (Principle 4b) deals with the case of changing the respobsibilities in the access control list of the clinical records. This part is represented as follow: a subject *s* of type responsible clinician wil be authorized to change the

responsibilities in the access control list of a patient clinical record if and only if he has obtained that patient's consent.

```
type
        auth+principle4b (subject <responsible_clinician> s,
                                target <ACL> clinicalRecordAcl,)
{
action changeResponsibility
if patientConsent (clinician,
newResponsibility) = "true"
        {
result = enable;
        }
}
```

Principle 5:

A subject *s* cannot delete any clinical record *r* untill this record expired *todayDate() > expireDate(r).*

Note that **when** is called the authorization filter and is used to restric an action by a given condition.

```
type
        auth-principle5 (subject s,
                                target <clinicalRecordAcl>r)
{
action delete
when todayDate() > expireDate(r);
}
```

Principle 6:

An audit record contains the subject identifier *s*, date *aDate* and time *aTime* of action, type of action *aType*, and the record that has been accessed *r* for all accesses on the clinical record *r* by a subject *s* must be created.

```
type
        oblig principle6 (subject s,
                          target <clinicalRecord>r,
{
on allAccess (s, aDate, aTime, aType, r);
do createAuditRecord (s, aDate, aTime, aType, r);
}
```

Principle 7:

Transferring data from clinical record A to clinical record B is not allowed unless all record in the access control list of b clinicalRecordAcl_B are included in the access control list of a clinicalRecordAcl_A.

```
type
        auth-principle7(clinicalRecordA,
                        ACL clinicalRecordAcl_A,
                        ACL clinicalRecordAcl_B,
          target <clinicalRecord>B)
{
action transfer (a.data,b.data) ;
when list(ACL clinicalRecordAcl_B)in
       list(ACL clinicalRecordAcl_A)
 }
```

Principle 8:

In the case of adding a new record (grant new user to have access to a clinical record) to a patient access control list, consequently the patient has to be informed at how many records the new user has access to.

```
type
        oblig principle8 (subject <responsible_clinician> s,
                          target <ACL>clinicalRecordAcl,clinician newName)
{
```

**on** addNew (newName,clinicalRecordAcl);

**do** informPatient (newName,

getNoAccess(newName));

}

### 4.7.4 Distributed Health Information System Specification Language (DiHIS)

The next language used to represent the 9 Principles of Security Policy Model in Clinical Information System is our proposed security language, DiHIS security specification language. DiHIS initiated to adapt the security policy for the dynamic environment of health information system. This language is using the Set Theory as the basis of representing each element within the system. It comprise of object which represent each organization in the HIS and subject which denotes the entity highly related with the particular object such as departments. These object divided accordingly to a different level. The highest object placed at the first level and so forth. In DiHIS, policy-based management applied to secure the connection among organizations in HIS. Below is description of DiHIS security specification language to represent the Anderson's 9 Principles of Clinical Security Principles.

Principle 1:

Let assume the system have a set of Authorized Entity represented as E. E might be individuals, roles such as doctors, nurses, researchers, and administrative staff. At the same time E could be a group of people working in a same department. The set of Authorized Entity represented as $E_g \equiv \{E_1, E_2, E_3, \ldots E_h\}$. E is associated with their respective clinical record that they are allowed to access under a name: Access Control List which denotes as $\Lambda$. The set of $\Lambda$ represented as $\Lambda_r \equiv \{\Lambda_1, \Lambda_2, \Lambda_3, \ldots \Lambda_p\}$ meanwhile the clinical record represented as $\Im$. The set of clinical record represented as $\Im_y \equiv \{\Im_1, \Im_2, \Im_3, \ldots \Im_n\}$. Where g, r, and y is a natural number that is greater than or equal to one and its infinity. The set $\Lambda \equiv \{(E_m, \Im_n)\}$ represents assignment of entity m to clinical record n.

Let assume there is an unknown entity as $E_o$ and $E_o$ request to access clinical record, the system will ask for the $E_o$'s identification. After the system received the ID from $E_o$, the system will check whether the entered ID is a member of the identification belongs in the E. If there is a match with identification of member of E, the system will recognized $E_o$ as a member of E, then the access is granted, unless the access is denied.

The figure below shows that only E is allowed to have an access to ℑ.

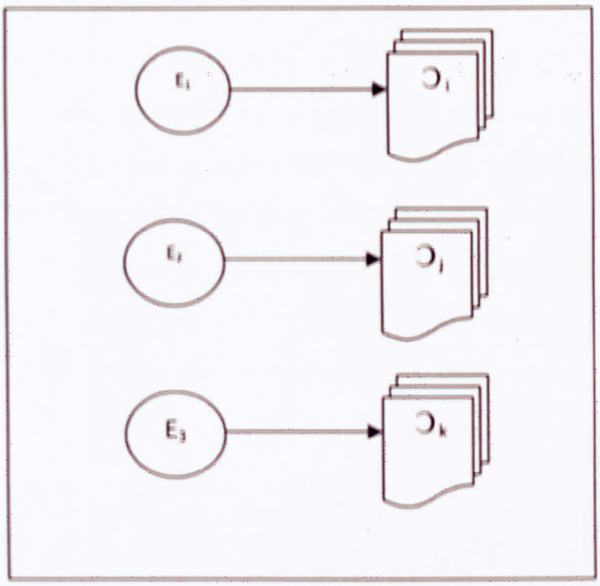


**Figure 14 Authorized entity access clinical record**

Below is how MAHIS represents the principle:

For a request access to a particular ℑ, the requestor (in this case, $E_o$) must be a member of Λ before his access granted.

If $E_o \in \Lambda$

$\perp E_o +\sigma \Im$

Else $E_o -\sigma \Im$

$+\sigma$ represents that $E_o$ has been granted access in Λ while $-\sigma$ depicts that $E_o$ has not been granted Λ.

Principle 2:

To represent this principle, here is an example. This principle is about who can access what. Only E allowed to access/ opens/ read/ append the ↄ that map to them. ↄ exists only after patient comes to the hospitals or clinics for a medical treatment. We will represent patient as Þ and a set of patient represented as $Þ_n \equiv \{Þ_1, Þ_2, Þ_3, \ldots Þ_d\}$ where n is a natural number that is greater than or equal to one and it's infinity. Meanwhile the clinician that entertained patient represented as Σ and a set of clinician represented as $\Sigma_m \equiv \{ \Sigma_1, \Sigma_2, \Sigma_3, \ldots \Sigma_c\}$ where m is a natural number that is greater than or equal to one and it's infinity. For the first the time a Þ undergo a medical treatment, his/her ↄ will be created inside that particular hospital or clinic. Then, the access list is assigned which Σ that can access which ↄ. In future, if that Þ comes again for medical checkup, his ↄ will be updated by that authorized Σ only.

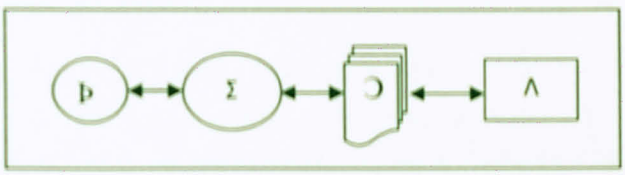


**Figure 15 Access control mapping**

In the figure 15 above, it shows access control mapping. We must understand that, access control cannot be created unless clinical record is existed. In order the clinical record to exist patient must come to see the clinician first before the doctor can entertain a patient.

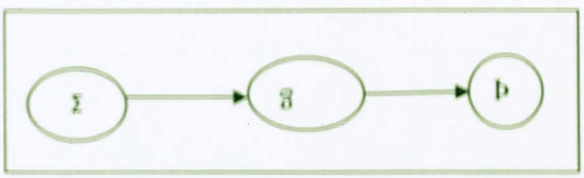


**Figure 16 Referring clinician flow**

Assume the patient need to be referred to another clinician. This process can only happen when the current clinician that treating that patient allowed this referring operation to

happened. The referring clinician represented as $\mathfrak{g}$ and a set of referring clinician will be represented as $\mathfrak{g}_u = \{ \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3, \ldots \mathfrak{g}_r \}$ where u is a natural number that is greater than or equal to one and it's infinity. After the clinician refer his patient to referring clinician, then that referring clinician also added to patient's clinical record access control list.

In other word, that both clinician and referring clinician are inside that patient's access control list where clinician and referring clinician are also members of E. +open is used to allow authorized entity to open the clinical record information. MAHIS representing this policy described below.

If $\Sigma \in \Lambda \wedge \mathfrak{g} \in \Lambda$

$\perp \Sigma \wedge \mathfrak{g} \leftrightarrow$ +open $\supset$

$\mid \Sigma \subseteq E \wedge \mathfrak{g} \subseteq E$

Principle 3:

This principle stressed about assigning one responsible clinician that will manage the access control list in one department. The set of department is $\mathfrak{h}_m = \{ \mathfrak{h}_1, \mathfrak{h}_2, \mathfrak{h}_3, \ldots \mathfrak{h}_t \}$. The term manages refers to access control list operations that are update, add, and delete the entity involved within access control list. These operations execute by one clinician who assigned as responsible clinician among the clinician name within the access control list.

Assuming the responsible clinician represented as $\Re$ and the number is strictly one and $\Re$ must be a member of the access control list. In case the responsible clinician is away, he can always delegate his job to another trusted $\Sigma$. This delegate issue is not main discussion so we will proceed with this policy.

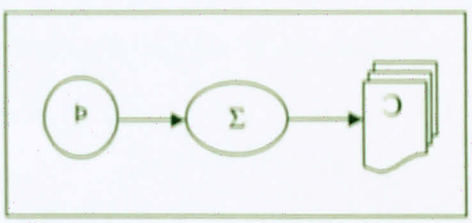


**Figure 17 Create record**

This principle commence when a new clinical record have been created. In figure 17 above, it shows how the flow of creating clinical record. After patient meet doctor, his clinical record will be created.

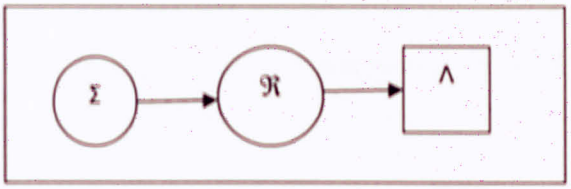


**Figure 18 Clinician inform responsible clinician**

Figure 18 shows this operation. When there are changes to clinical record, clinician must inform the responsible clinician about this newly added clinical record. Responsible clinician will then add the newly added clinical record into the existing access control list as well as the E information. From the scenario in principle 2 where a clinician approved referring clinician, the clinician must inform responsible clinician about the newly added referred clinician so that his information can be added into that particular clinical record's access control list.

$\Re_n \equiv \{\Re_1, \Re_2, \Re_3, \ldots \Re_i\}$

If $\Re_i \in \Lambda \wedge \Re i \in \Re_n$

$\perp \Re_i$ +(alter,append) ~ $\Lambda$

| number$[\Re_i] \in \underline{\mathrm{D}}_i \equiv 1$

Where $\Re_i$ represents responsible clinician for department i. The +(alter,append) implies the responsible clinician allowed to perform operation alter and append which this operation apply for access control list. The term applies represent with the symbol ~. And number$[\Re_i] \in \underline{\mathrm{D}}_i \equiv 1$ represents the number of responsible clinician which belongs to one department is strictly one.

Principle 4:

This principles discusses about the task that performed by authorized clinician to the clinical record that belongs to his access control list. The tasks are open and update

the clinical record and transfer the access control to another clinician. The policy stated that responsible clinician must notify the patient which his/ her clinical record has been updated by the authorized clinician. Logically, if the responsible clinician didn't know what the clinician done; he will not inform anything to the patient. That why we will assigned the clinician to inform responsible clinician after they have perform some update operation to the clinical record. Figure 19 shows the clinician update information in clinical record.

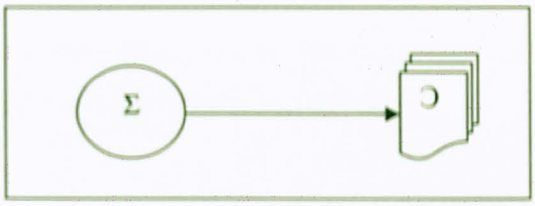


**Figure 19 Clinician update clinical record**

Responsible clinician after received notification from the clinician will then obligated to inform the patient of which his/ her clinical record is updated. But before this to happened, the responsible clinician must identify whether this is an emergency or common situation. In common situation, responsible clinician will inform the patient about the operation had been made to his/ her clinical record and he waits for the concern from the patient. Figure 20 shows this operation.

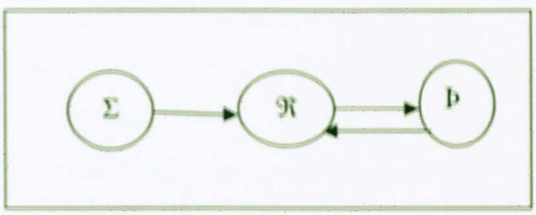


**Figure 20 Consent Flow**

If it is an emergency case, responsible clinician is obligated to notify the patient about the operation has been done to his/ her clinical record without need to wait for patient's consent. Clinical records assignment to which particular patient represented as PR = {($Ↄ_i$, $Þ_j$)}.

Below is the principle represented by MAHIS.

$\int \Im_i$ (open, add, transferResponsibility)

$\perp \Re_n$ +(informÞ) $\wedge$ +(obtainÞConsent)

$\vee$

| Emergency

$\perp \Re_n$ +(informÞ) $\wedge$ −(obtainÞConsent)

| Þ $\in$ PR

| $\Im$ (open, add, transferResponsibility) means clinical record will be opened, new record will be added and change in responsibility will be made.

Principle 5:

This principle stressed that only authorized user can delete the old clinical records when the records have reached the date of expiry. To perform this principle, E must have the authorization to perform the delete operation as well as have the ability to access the old clinical records. For this person to know that the old records have reached the expired day, it must be informed by the system. Here it means that the period of living of the clinical record must be stated in the computer system at the first day it was 'born'.

The system must indeed have a counter function that will count and provide notification when the expired data is reached. In addition, it must have a very proper notification process, the system must keep notifying until it received a respond from authorized user indicating that the message have been received. Adding to that the system must intelligent enough to know that the notification given to and getting the feedback from the E only. This is to prevent unauthorized access to the sensitive information.

Below is the MAHIS specification language representing the principle.

$\int D_{today} \geq D_{expiry\_date}$

$\perp$ E ☒[$\Im$,$\alpha$]

| E $\in$ $\Lambda$

| α denotes the system and ☒ represents that delete access has been granted to entity E when the system date is equal or greater than expiry date.

From this principle, the author found that the principle is not compatible with nowadays distributed system procedures. Everything must be done fast and automatically. Supposedly the system notifies several days earlier before the exact date of the expiration, the authorized person can plan to perform deletion task in an arranged way. For instance, if the E knows in advance the expired date, he/she can set the system to automatically perform the deletion process on the expired date. This is the most convenient way to prevent any missed dateline or the absent E to respond to the notification by the system.

After the authorized user received the notification, it will then perform the deletion. This deletion process' information will be store in the computer system and this history can be the reference in the future such as for an audit trail.

Principle 6:

This principles stressed on the recording the access operation. The last sentence in this policy "*an audit trail must also be kept of all deletions*" has similarity with the previous policy.

In this policy, the author assumes that the login operation is successful and the requestor is approved as valid member of E, allowed to access clinical record that is mapped to him. Every clinical record must have Archive which consists of all the information related with the access operation. Each clinical record access will have its own set of Archive denotes as $\tilde{a}$. The set of Archive represented as $\tilde{a}_n \equiv \{\tilde{a}_1, \tilde{a}_2, \tilde{a}_3, \ldots \tilde{a}_f\}$ where n is a natural number and greater than or equal to one and its infinity. Each $\tilde{a}$ consists of several numbers of subsets. There is the set of identification (ID) of the E that accesses the clinical record represented as $E_{ID}$. The sets of time access login and time logout. The set of period of the access and the set of task performed by the E towards the clinical record. The task performed could be open, read, write, update, delete, copy and print. This information saved into the Archive every time clinical record is accessed.

The access date denotes as $D_{access}$ and the set of $D_{access}$ represented as $D_{access\ y} = \{D_{ac\ 1}, D_{ac\ 2}, D_{ac\ 3}, \ldots D_{ac\ s}\}$ where y is a natural number and greater than or equal to one and its infinity. Access time represent as $t_{access}$ and the set of $t_{access}$ represented as $t_{ac\ x} = \{ t_{ac\ 1}, t_{ac\ 2}, t_{ac\ 3}, \ldots t_{ac\ v}\}$ where x is a natural number and greater than or equal to one and its infinity. Meanwhile logout time represent as $t_{logout}$ and the set of $t_{logout}$ represented as $t_{logout\ p} = \{ t_{lo\ 1}, t_{lo\ 2}, t_{lo\ 3}, \ldots t_{lo\ z}\}$ where p is a natural number and greater than or equal to one and its infinity. Access duration represent as $t_{duration}$ and the set of $t_{duration}$ represented as $t_{duration\ i} = \{ t_{dur\ 1}, t_{dur\ 2}, t_{dur\ 3}, \ldots t\_dur\ n\}$ where i is a natural number and greater than or equal to one and its infinity . The tasks that could be performing by the E are represented as a set of operation, Task = {read, write, update, delete, copy and print.}

We need to understand that this operation is not an operation performed by the clinician or people, it is a system operation. Below is the figure representing the above situation.

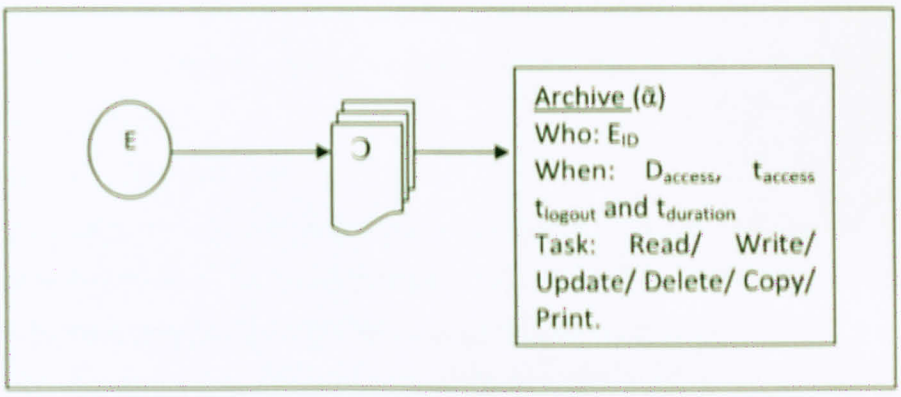


**Figure 21 Create archive**

Below is the DiHIS security specification language representing the policy.

$\bar{a}_i = \{E_{ID} \cup D_{access} \cup t_{access} \cup t_{logout} \cup t_{duration} \cup Task\}$

Archive maintains the complete operation history at any instant. $E_{ID}$ represent the person who performed operation on the clinical record. $D_{access}$, $t_{access}$, $t_{logout}$, and $t_{duration}$ denotes the day and time respectively when the operation is performed. Task depicts the task performed by the E.

Principle 7:

Firstly, we are going to tackle the tail of this principle where is sound like this "*if and only if B's access control list is contained in A's.*"

*If and only if* is represented by this symbol ⇔.

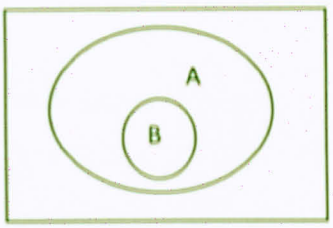


**Figure 22 Subset**

The term *access control list B contained in A* just like a subset. It can be interpreted that set B is a subset or equal to a set of A. This sentence represented as $B \subseteq A$. Figure 22 shows B is a subset of A.

That brings us to this: $\Leftrightarrow B \subseteq A$.

Secondly, to cater the head of the principle "*Information derived from record A may be appended to record B*". This sentence interpreted as record A can be added to the end of record B. In other meaning, A added to B. In set this represented as $A \cup B$.

In addition, we added a variable x to represent the whole operation.

That brings us to the representation: $x \equiv ( A \cup B \Leftrightarrow B \subseteq A)$

Principle 8:

To help describe the policy, this is a scenario created for better understanding. Assume that a clinician have a list of accessed record denotes as LR. This list is obligate to each clinician. As soon as clinician has been granted to access a particular clinical record, that clinical record must be added into the clinician's access list.

When clinician requests to access another clinical record, then, it must first request to responsible clinician. Responsible clinician will then ask from the clinician to present his LR. Clinician gives away the list to the responsible clinician for evaluation.

We will assign a variable to represent the number of accessed record list as value y. It also assume here that the system has set the maximum number of accessed record list that is acceptable for each clinician, z. If the evaluation finds that value y of clinician has exceed or equal to the value z, then the responsible clinician will send notification to the patient stating the clinician who has a lot access list is requested to access his clinical record. Patient then sent feedback to the responsible clinician whether give consent or not.

Below is the figure representing the process.

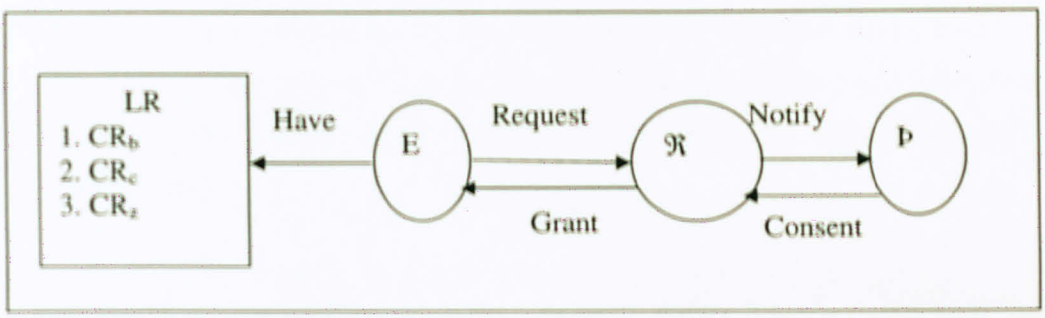


**Figure 23 Principle 8 explanation**

Below is the DiHIS security specification language representing the policy.

$| \Sigma_j \notin \Lambda_i$

$\int \cup [\Sigma_j , \Lambda_i]$

$| \Re_n \in \Lambda_i$

$\perp \Re_n$ +(informÞ) $\wedge$ +(obtainÞConsent)

$| \Sigma_j$ – number[$\Im$] $\in \Lambda \geq$ numberMax

Principle 9:

We will be describing this principle with a scenario. Let assume there is a computer system and we represent it as $\alpha$. The set of computer system will be represented as $\alpha_n = \{\alpha_1, \alpha_2, \alpha_3, \ldots \alpha_t\}$ where n is a natural number that is greater than or equal to one and it's infinity. There is also the subsystem which represented as $\beta$. The set of subsystem will be represented as $\beta_m = \{\beta_1, \beta_2, \beta_3, \ldots \beta_k\}$ where m is a natural number that is greater than or

equal to one and it's infinity. The independent expert in this scenario assumed as systems that evaluate the effectiveness of the policies been performed and denote as δ. The set of independent expert represented as $\delta_k = \{\delta_1, \delta_2, \delta_3, \ldots \delta_o\}$ where k is a natural number that is greater than or equal to one and it's infinity. The policy been enforced will be represented as P. A set of policy will be represented as $P_q = \{P_1, P_2, P_3, \ldots P_c\}$ where q is a natural number that is greater than or equal to one and it's infinity. The scenario start when α want to perform a task that requires policy enforcement. If β to enforce the policy, it must know what type of task to be performed by α. So, firstly, α must send a request R representing the task that it's going to perform to β. The set of R is represented as $R_j = \{R_1, R_2, R_3, \ldots R_m\}$ where j is a natural number that is greater than or equal to one and it's infinity. α also required to send a copy of the same request R to the δ. Figure 24 describes the scenario.

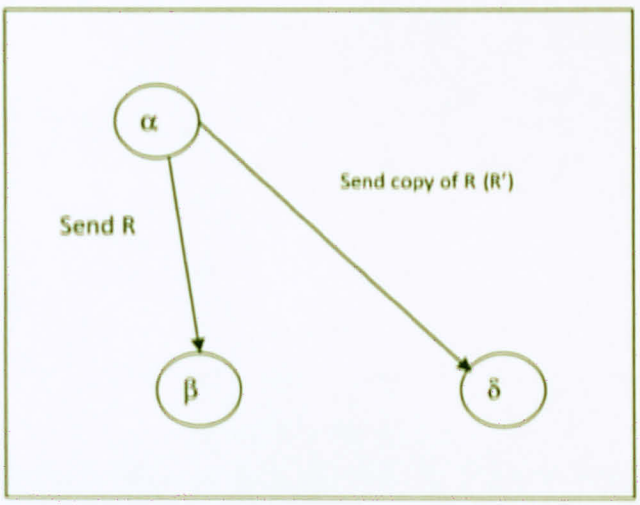


**Figure 24 Send Request**

After both subsystem received the request R from α, the next step explain below because it happen concurrently.

In β: β will then enforce the policy, P.

In δ: δ will then do the process calculation internally of finding the correct value of what suppose to be the result of the request R. This expected value processed by δ will be represented as P#. The set of expected value will be represented as $P\#_t = \{ P\#_1, P\#_2,$

$P\#_3, \ldots P\#_t\}$ where t is a natural number that is greater than or equal to one and it's infinity, δ then wait for value resulted of the performed task from α.

After β enforced the policy and α allowed to perform the task it requested earlier R. After completing the task, α will have value after task performed represented as P-. The set of value after task performed represented as $P\text{-}_f \equiv \{ P\text{-}_1, P\text{-}_2, P\text{-}_3, \ldots P\text{-}_y\}$, where f is a natural number that is greater than or equal to one and it's infinity.

α must send P- to β and at the same time send a copy of P- to δ.

β will save P- into its record for the proof that task is complete and the policy is enforced. It then waits for another request performing task. This process describes in the figure 25 below.

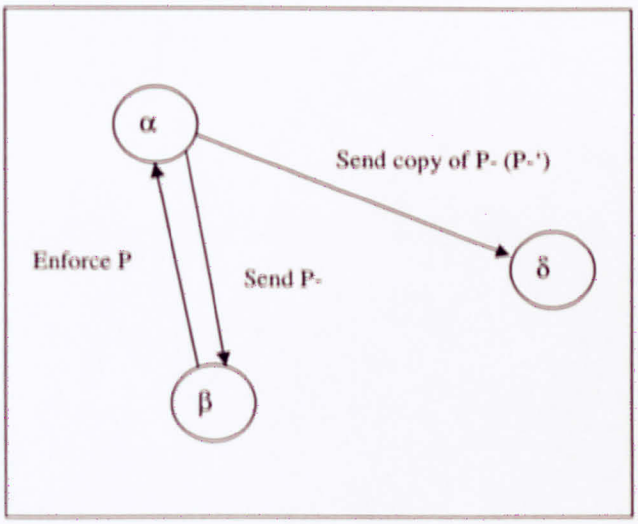


**Figure 25 Compare value**

δ on the other hand, is going to compare the value of P-' with P#. If the value is same, the δ can conclude that β is enforcing the policy effectively and correctly. But if the value is not same, δ will have to update the β so that the same mistake will not be repeated again.

Let assume that δ have received R and waiting for the P- from α. But it never received any value from α. How long δ will keep waiting for the result from α. Then there must be allocated a maximum time period for performing task and time waiting. This time must be acceptable for α that it will have enough time to perform the task and time to send the value to both δ and β. The time waiting represented as tw meanwhile the maximum time

period for performing task represented as tMax. If the tw in δ has exceed tMax, δ must ask justification from β. Any error must be updated in β.

If δ received R from α which is not valid or an error, it will ask justification from β. β then must be updated to overcome this error so that the system will not meet a deadlock. It crucial to correct β every time there is an error or unidentified value received by δ. β is responsible to enforce the correct policy and so it must behave. δ is just a reviewer and it will issues a query if something doesn't happens as planned or unexpected event occurs. An important reminder here, this process is not process perform by person or clinician. This whole process will performed by the computer system.

This situation presented by DiHIS- security specification language below in step by step:

α: send (β, R)

α: send (δ, R')

β: receive (α, R)

δ: receive (α, R')

δ calculate the expected result of R'. The expected result denotes as P#

β: $P_i \rightarrow \alpha \mid P_i \in P$

α: send (β, P-)

β: receive (α, P-)

α: send (δ, P-')

δ: receive (α, P-')

δ: compare (P#, P-')

If P# ≡ P-'

Then OK

Else send (β, Notify_message)

$\mid \beta: P_i \rightarrow \alpha \mid P_i \in P$ denotes the subsystem is enforcing the policy i to computer system where the policy i is a member of policy (P).

### 4.7.5 The Outcome

Although all the above languages basically targeting specifying security policies, they focus on different aspects, for instance ASL focuses more on the access control policies

and LaSCO attempt to express constraints on objects, while Ponder aims to specify security and management policies for distributed systems. Additionally, they are different from the language's character point of view. Whereas ASL based on logic and LaSCO policies are specified as logical expressions and as directed graphs, Ponder is a declarative language inheriting its syntax from the OCL "Object Constrain Language". According to the nature of each of these languages, we have found that some of Anderson's principles are not representable. For example, principles such as those concerning auditing operations (i.e. Principle 6) and control aggregation problems (i.e. Principle 8) were not representable by ASL and indirectly expressed by LaSCO. On the other hand, Ponder was more suitable for those kinds of principles since Ponder has got forms to deal with the management policies. As for DiHIS, this language able to represent all the principles explicitly. The comparison of these four languages presented in Table 1 below. Table 1 illustrates the comparison between these four languages according to their ability to express Anderson's clinical security principles.

| **Principles /Language** | **ASL** | **LaSCO** | **Ponder** | **DiHIS** |
|---|---|---|---|---|
| Principle 1 | ✓ | ✓ | ✓ | ✓ |
| Principle 2 | × | ⚠ | ⚠ | ✓ |
| Principle 3 | ⚠ | ✓ | ✓ | ✓ |
| Principle 4 | ⚠ | ⚠ | ✓ | ✓ |
| Principle 5 | × | ✓ | ✓ | ✓ |
| Principle 6 | × | ⚠ | ✓ | ✓ |
| Principle 7 | × | ✓ | ✓ | ✓ |
| Principle 8 | × | ⚠ | ✓ | ✓ |
| Principle 9 | × | × | × | ✓ |

**Table 1 Comparison table shows how far ASL, LaSCO, Ponder and DiHIS language can represent security policy model in clinical security principles**

Legend:
Not applicable = ×
Explicitly Represented = ✓
Indirectly Represented = ⚠

DiHIS is a language initiated especially for distributed health information system that covers all aspects of access right. Even though the language able to represent all the principles explicitly, however the main features of this languages where it covers the changeable part still not tested and proved. This part will be discussed in depth in Chapter 5 where the real life case study involving Malaysia National Health Information System is used to see the applicability of DiHIS.

# CHAPTER FIVE

# APPLICATION DOMAIN

In this chapter, a prototype presented as case study of connection among organizations or organizations within distributed HIS. We have created an imitation of shared clinical records between agents within the network. Security policies that should be used during this process are discussed. This prototype made up so that it will carry out the 9 principles of security model of clinical information system (Anderson Jan 1996; Anderson May 1996) including policies that are crucial for a distributed HIS.

## 5.1 Prototype Overview

The distributed HIS itself consists of many organizations such as schools, universities, colleges, research organizations, hospitals, clinics, labs, insurance companies, employers, district health offices, states health departments, health ministry and the public. The organizations were grouped into a dotted box which represents the internal entities of the HIS. The schools, universities, colleges, researcher bodies, insurance companies, police and attorney organizations, and companies/ employers can be represented as external entities that wish to access the information from HIS.

Relationships among these organizations are shown below.

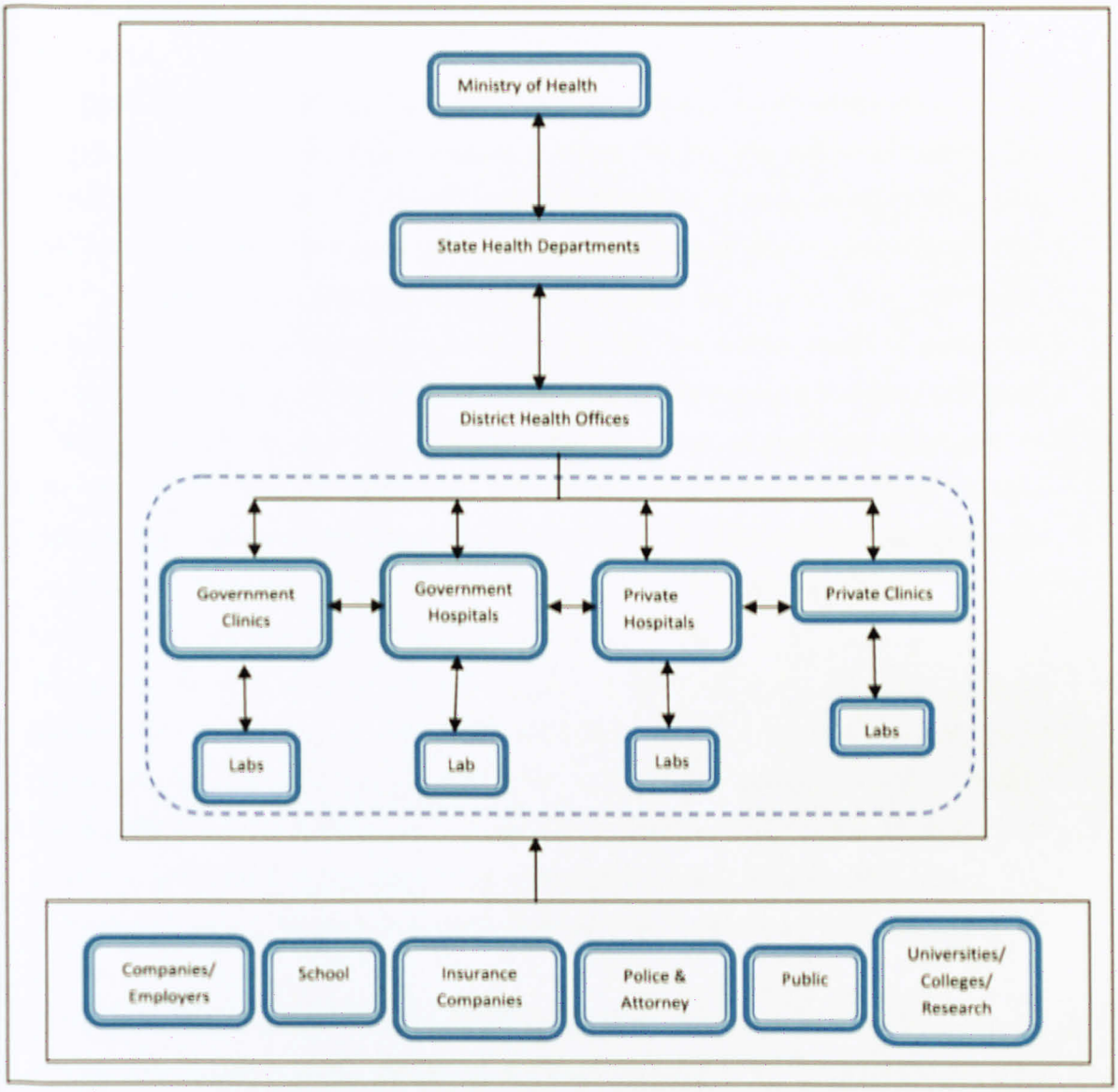


**Figure 26 Distributed HIS Application Domain**

The arrow shows direct relationship that occurs among these agents. Each agent will have its own databases which stores theirs' organization confidential clinical and administrative records. The suitable protection must be carried out by the agents in order to protect their records from being accessed by unauthorized person. This protection will be carried out by the HIS officers. The HIS officers will be allocated at each organization which carry responsibility to control all the transaction traffic within these organizations.

The transaction must be conducted with their acknowledgement and approval only. The number of authorized person is limited and the transaction can be executed in trusted conditions.

The main issue of health care network is to able personal health information sharing among the agents securely. It is important to ensure the integrity and availability of the information at the time it's needed and transferred in a very secure, trusted and convincing procedure. Not to forgot only authorized person can request and received these information. A connection happens, when there are two or more agents are exchanging something with agreement from each side. The entities would be; entity that has the information (provider) and entity asking for the information (requestor). Both of them can become requestor and provider at the same time. In fact, they must agree to provide some information before they allowed requesting information. There must be also existing information that can be transferred. The information must be updates always in order to ensure only the latest information circulated within the network. This is crucial to support the integrity of the information.

We suggested that, all the agents within the network must come to an agreement on what information rationale to be shared. To determine what type of information, each organization is obligate to provide their list of needed information and the justification. Having this, it will be distributed so that every agent within the HIS and acknowledged by others. With this, they can come to an agreement of what is the acceptable information to be shared and at the same time they must provide the information needed by other agents.

Afterwards, there's a must for each agent in the health care network to build their own system. This system acts just like an intermediate for them to share within the network. The system implemented must be equipped with suitable security enforcement. It is crucial to have trusted HIS officer that will handle and take care of the system. This trusted HIS officer also will be the intermediate person that handles transaction during sharing personal HIS is executed.

Derived from this figure, we have listed the connection for each of them.

- Ministry of health (MOH) represents the reference for the whole units that working in medical field.

- Some entities have a direct interact with MOH while others must interact through intermediate entities.
- Health State Department at each state has direct relationship with MOH.
- Each District Health Offices has direct relationships with its Health State Department.
- The internal entities in each district have direct relationship to their District Health Offices.
- The internal entities in each state need to connect with the State Health Department through their Direct Health Offices.
- The internal entities in each state have direct relationship to own labs.
- The external entities interact directly with any of the organizations within the internal entities.
- The external entities interact with State Health Department through District Health Office.
- The external entities interact with MOH through the State Health Department.
- There will be internal connections among the internal entities. It means each of government hospitals, government clinics, private hospitals, private clinics, and labs have interaction with each other.

In the next section, we will group each of the organizations stated in Figure 26 following DiHIS diagram (Chapter 4). The policies involved will be discusses and DiHIS security specification language will be used to represent all the policies that have been derived from this section.

## 5.2 Using DiHIS Security Language to represent the application domain

Diagram below shows organizations as in the prototype applied to DiHIS diagram. We have assigned the Ministry of Health which denoted as MOH to be at the highest level. The State Health Department which denoted as SHD is placed a level below MOH. Meanwhile, the DHO, District Health Office which denoted as DHO is at the third level from MOH. At the last level, there are the organizations which fall under Internal and

External Entities. We placed each of this organization according to their functionality and importance.

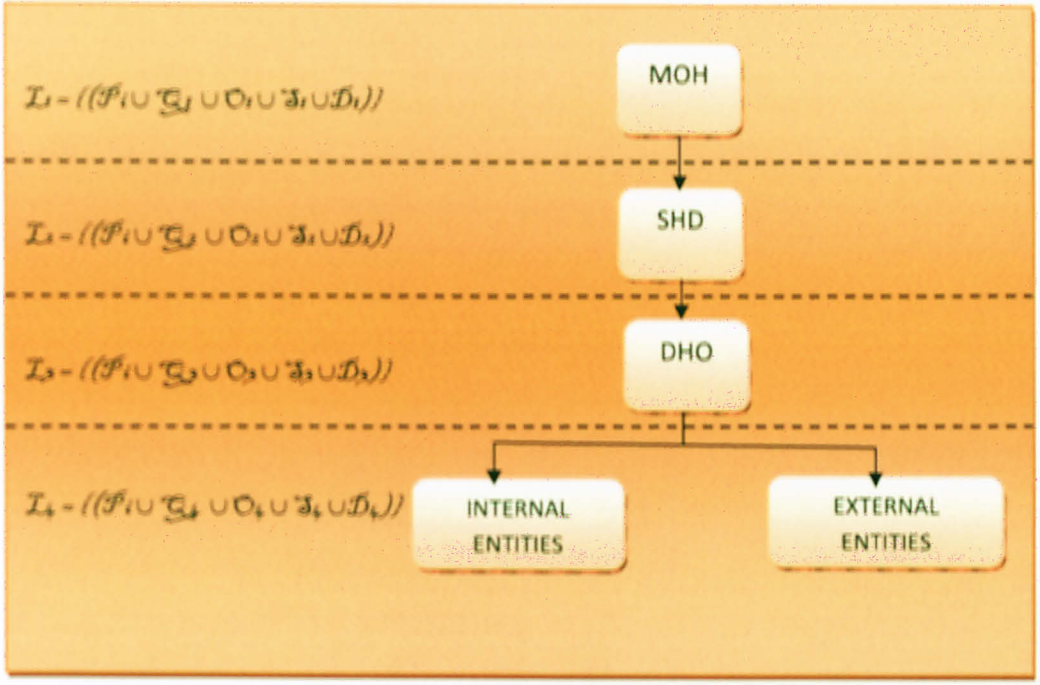


**Figure 27 Diagram distributed HIS applied in DiHIS diagram**

As we can see the $\mathcal{I}_1 = ((\mathcal{P}_1 \cup \mathcal{C}_1 \cup \mathcal{O}_1 \cup \mathcal{A}_1 \cup \mathcal{D}_1))$ denotes that in Level 1, it has several subset of; a set of public policy, set of sub policy which unique to the respective level, set of objects that belong to the respective level, set of subjects that belong to the respective level, and set of additional policy that belongs to the level's subject. These subsets reside at each level and can be recognized depending on which level they belongs to. The public policy is the policy that applies to all level which denote as $\mathcal{P}_1$.

Public Policy in the case study:

- Each entity would need to go through the entity below its level until it reaches the requested entity, unless the requested entity is just one level below, then, it have direct access. This direct access mean entity located below one level of the requestor is assigned the access control. This access control denotes as ACL. The target entity denotes as Et. The target entity at another level denotes as $Et_1$. This policy named as $\mathcal{P}_1$.

  If Et ∈ ACL

E +(access) Et

Else E request access $Et_1$

- Policy above can only be over write in case of emergency following the need to know policy.

  The Need to Know Policy will be denotes as $\mathcal{P}_2$.

  ◈ Emergency

  $\mathcal{P}_2$ +(override) $\mathcal{P}_1$

### 5.2.1 Government and private clinics and hospitals

Below is the model of information sharing between two HIS system that are located at different location. The diagram below shows how the connections are. It also shows how sharing clinical record should be performed by the authorized person.

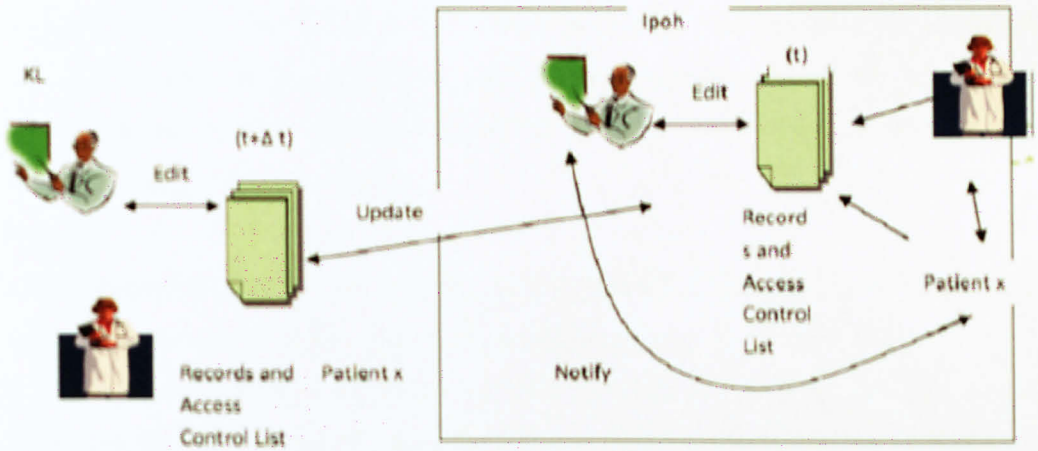


**Figure 28 Sharing clinical record by the authorized person**

Below is the policies derived from the connections among both government and private clinics and hospitals and labs.

Requirements

1. HIS unit in both private and government hospitals and clinics must be established.
2. Records must be created for patients in both private and government hospitals and clinics and saved in the HIS units.

3. The HIS operators assign the list access control whereas both the clinician who may open the record along with the patient must be included in the access control list.
4. Records must be shared between the HIS Units so record can be accessed wherever and whenever the same patient is being admitted, updated records must be distributed again to all HIS Units.

HIS Units in both government and private units must be established, a HIS person is the only one who can edit the patient record besides assigning the authority for access control list. Patient updated records must be distributed to all HIS Units. Patient must be aware of any modification, authority transfer, and record accessed. HIS person in each unit will be represented as H.

Trusted HIS person in this system represented as H. H become the responsible person who will take care of the access control list. Access control list contains information about the clinical records belong to the patient along with their clinicians that are authorized to access the records. The system assume that only the patient, the responsible clinicians can have the access to the clinical record. In case any changes in the access control list such as adding a referring clinician to a particular clinical record can only be executed by the H. The reason is to uphold the integrity of the clinical records by limiting the number of person can access it.

$H \leftrightarrow CR$

Above statement denotes that only and only if HIS person request accesses the clinical record, access is granted. Any request from other entity must be through H.

H is obligate to perform some operation based on different situation. In case of opening record by the clinician toward the clinical record that he is allowed to access must be under knowledge of H. Besides that, if there are adding referring clinician into the access control list, H must be informed and H is the only authorized person who must perform the addition operation. Not the clinician itself. This restriction can prevent clinical records being accessed by too many clinicians. H also obligated to inform patient if any of these cases occurs. The consent of the patient must be obtained. But, in case of emergency, the patient consent is not a must. These policies represent as below:

$\int \mathcal{O}i$ (open, add, transferResponsibility)

$\perp$ $H_n$ + (informÞ) $\wedge$ + (obtainÞConsent)

$\vee$

| Emergency

$\perp$ $H_n$ + (informÞ) $\wedge$ − (obtainÞConsent)

| Þ $\in$ PR

PR here denotes that the set of clinical record m belongs to patient n. PR = {($Ↄ_m$, $Þ_n$)}

Adding to that, if any clinician is to be added into an existing clinical record, he/she must informed H his/her list of accessed record. List of accessed records stating a number of access controls that already granted to the clinician. H will then notify the patient about the clinician who already has too many accessed control that wish to add that patient clinical record in his access control list. H must then wait for the patient consent. The policy represented as below.

| $\Sigma_j \notin \Lambda_i$

$\int \cup [\Sigma_j , \Lambda_i]$

$\perp H_n$ +(informÞ) $\wedge$ +(obtainÞConsent)

| number[Ↄ] $\in \Lambda \geq$ numberMax

| Þ $\in$ PR

The $\Sigma_j$ denotes as the doctor that request to add access control list.

In case of sharing, transferring and updating clinical records, this how the process should be executed. Let us assume that a patient X who is originally treated at a hospital in Ipoh getting a treatment in hospital in Kuala Lumpur. Patient X's clinical records are situated at the site system in hospital in Ipoh. Let assume that this patient X went to KL and he meet an accident. When he is being treated at hospital in Kuala Lumpur, H in hospital Kuala Lumpur will request patient X's clinical record from H at hospital in Ipoh. The question is how H in KL knows to request directly from H Ipoh? If patient X is conscious, he can inform the clinician, but how to do if patient X in unconscious and can't provide any helpful information. This is the issues that need to solve. Creating a card for each patient for them to store the history clinical record has been famous application in (Bernd Blobel 2007).

H at hospital in Ipoh will received the request from H at hospital in Kuala Lumpur. Let assume H at hospital in Ipoh as H_Ipoh and H at hospital in Kuala Lumpur as H_KL. H_Ipoh first need confirm the identity of the requestor. H_KL will then provide his identity and then, can proceed with the request. H_Ipoh will then make a copy of the patient X clinical record and send it to the H_KL. This copy of the record and sent clinical record must be marked at the patient X clinical record and recorded into an archive. The archive will capture the date, login and logout time, task performed, between who and who. This process is crucial to perform especially when an audit trail conducted, these records will be used as a proof.

After H_KL received the copy of the clinical records from H_Ipoh, he will forward it to the clinician in charge. H_KL also will add the clinician's name in KL inside the access control list for Patient X. H_KL will delegate clinician in KL to access the clinical record in a given time frame, that as long as the patient is treated in KL. The clinician in KL will update the patient X's clinical record and send to H_KL. H_KL then distribute the updated record to all H in the system. Only the update information on the clinical record will be distributed among the network. This is to ensure the clinical records are always available at any time it's requested.

Below is the representation the policy:

| H_KL ∉ Λ

⊥ H_KL request + (access) $\mathcal{O}_i$ ⇨ H_Ipoh

| H_Ipoh ∈ Λ

⊥ H_Ipoh delegate H_KL ⇨($\mathcal{O}_i$), (+access), ($t_{duration}$)

H_Ipoh send $\mathcal{O}_i$ (t) = [Þi, Σj, H_Ipoh] ⇨ H_KL

H_KL +(update) $\mathcal{O}_i$ (tϒ+Δt) = [Þi, Σk, H_KL]

⊥ H_KL send μ ⇨ ∀H

H_Ipoh delegate H_KL ⇨($\mathcal{O}_i$), (+access), ($t_{duration}$) represent HIS person in Ipoh delegate the access of clinical record patient X to the HIS person in KL stating the type of access he can perform and the duration of the delegate valid. After HIS person in Ipoh has delegate the access to HIS person in KL, then the clinical record can be send to KL.

H_Ipoh send $\Im_i(t)$ = [Þi, Σj, H_Ipoh] ⇨ H_KL denotes that HIS person in Ipoh send a copy of clinical record i at time t containing information patient i, doctor that authorized to this patient and location on data in Ipoh to the HIS person in KL.

Where μ is the updated $\Im_i$ which represented as $\Im_i(t\Upsilon+\Delta t)$ = [$Þ_i$, $\Sigma_k$, H_KL].

The Δt denotes as the updated time that H_KL update the clinical record. The $\Sigma_k$ denotes that doctor treat the patient i in KL has been added into the doctor that authorized this clinical record and the H_KL denotes HIS person is from KL.

$\int t\Upsilon \leq t_{duration} \leq t_{expiry}$

$\perp$ H_KL +σ

Else H_KL -σ

This denotes that the during the time duration, HIS in KL will be allowed to perform the access, if the expiry time has approach, then the access denied.

As stated in the security policy model in clinical information system, each transaction executed must be logged into archive for history retrieval. The archive must be logged at both HIS location involved which are KL and Ipoh.

H_Ipoh = { H_Ipoh ∪ H_requestor ∪ $D_{access}$ ∪ $t_{access}$ ∪ Task ∪ $D_{delegate}$ ∪ $t_{delegate}$ ∪ $E_{ID\_delegate}$ ∪ +access_delegate ∪ $t_{duration\_delegate}$ ∪ $t_{logout}$ ∪ $t_{duration}$ }

The archive in Ipoh will store information such as the date and time HIS person access the system, between who they interact (in this case HIS in KL) the task he perform, to whom delegation goes to, the date and time of the delegation process, what access allowed to be executed by the delegation receiver, the time duration for the delegation is valid, as well as the logout time and duration of access by the HIS person in Ipoh.

ã_KL = { $^{\tau}$H_KL ∪ $^{\tau}$H_receiver ∪ Daccess ∪ taccess ∪ Task ∪ Dreceived_delegate ∪ treceived_delegate ∪ EIDdelegate ∪ accessAllowdelegate∪ tduration_delegate ∪ tlogout ∪ tduration }

The archive in KL will store information such as the date and time HIS person access the system, between who they interact (in this case HIS in Ipoh) the task he perform, from whom delegation comes from, the date and time of the delegation process received, what access allowed to be executed by the delegation receiver, the time duration for the

delegation is valid, as well as the logout time and duration of access by the HIS person in KL.

Above are the sharing processes among H units that heavily need the clinical record information in their daily work. Not to forgot that in a distributed HIS there are multi agents involved. And above situation can be executed by both government and private hospitals and clinics including the external entities (for instance insurance companies, employers, and each of these agents carries different task to perform and different needs. In order to show how these agents interact with each other, the author derived some policies that help these agents interact with each other in an arranged and secured procedures.

The author has been looking at each of the agents; capture their general and common task. From here, the author captured the agent requirement and needs from others in order to perform it task effectively.

### 5.2.2 Health Ministry

Looking at the health ministry scope of task, it is not wrong to say that their task is to come out with health care program throughout the country. From the interview conducted with the representatives from Ministry of Health of Malaysia, they said they have with them several level of reporting. The government clinics and hospitals are required to send monthly report to their district health office. Here, in district level, they will need to produce an executive summary which will be sent to the state health department. Here, in the state level, they will review all the reports and generate an executive summary before it can be sent to the health ministry. The private clinics and hospitals, at every end of month, they will be required to send a statistical report to the health ministry. In health ministry, there is one department that will cumulate all these reports and make them into a summary report from all units that will be used to evaluate the health quality and system. From this report, responsible in health ministry will decide the plan or next steps to be taken to overcome the stated problem or weaknesses.

Below is DiHIS representing the policy.

$\Phi D_{today} = D_{end\_of\_month}$

$\forall$ SHD send report $\Rightarrow$ MOH

This policy denotes that each entity obligate to send report to the MOH at every end of the month.

Besides the monthly statistical report, another way of connection between these hospitals with the health ministry is in case of emergency. It is a must and it's a must for any if these units that encounter epidemic cases, to report it to the District Health Office (DHO) immediately. This report can only be hit by an authorized and trusted person. This is crucial to prevent false alarm. After the report received from the unit, staff from DHO will investigate the reported case. At this moment, they will require the personal information about the victim such as the address, working place's address, medical history and any relevant information. In this case, we have to implement the Need To Know Policy.

Need To Know will allow an authorized person to access certain allowed clinical records to be used for him to perform a special task. This will include the time period of access; the release time and expired time. It also important to assure that the person who is performing this need to know task will guarantee to restrict the use of this information for the specific task only. Figure 29 shows a connection between hospital and Health Ministry where the situation that bring to the Need To Know policy.

In order to judge the need to know performer is doing the accurate task with the granted access information, audit trail will be performed. Here, the ninth principle of security model for clinical information system (Anderson Jan 1996; Anderson May 1996) take places.

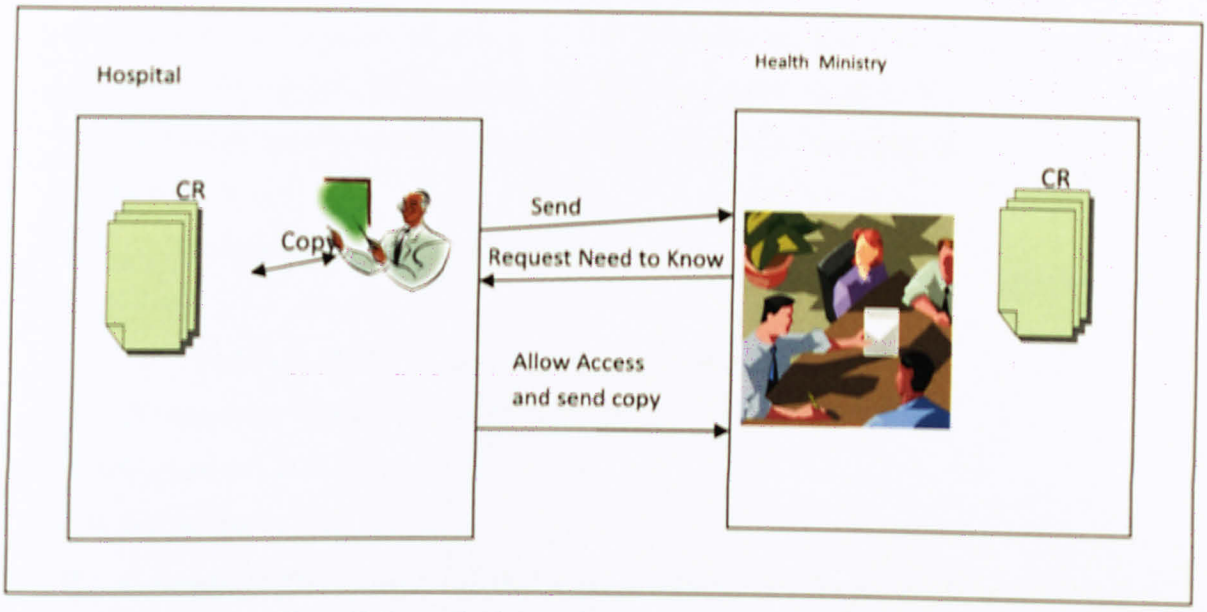


**Figure 29 Connection between hospitals and health ministry**

In finding the best solution for the need to know problem, the access granted will be given only to a predetermined task. There would need to be an agreement between information provider and the need to know requestor. With the stated agreement, it would easy to determine what task allowed in need to know policy. With the acknowledgement of the tasks are, it easy to set the time frame for the task to be performed. The expired task also can be determined as well as the information size. Knowing the information size helps the information provider preparing the appropriate method to transfer or sharing the needed information. There also need to have the guarantee to restrict the use of this information only by the specified task.

Usually, a connection between MOH with its lower level entity depends on report send by these entities to the MOH. In MOH there is one department called Disease Control Division (DCD) which they claim they would need to have this need to know ability for emergency cases. The figure above show the first arrow from hospital to MOH labeled 'send'. It indicates hospital send report to the MOH at some point in unusual cases happened. The respond from MOH is to ask for the detailed information that resides in that particular hospital. Here, the need to know policy applies. This policy has similar method with the delegation policy. Assume the process of need to know happened

between MOH and Government Hospital (GH). Each of this entity has its own HIS person. The request will be executed between these two persons. Firstly, the HIS person in MOH will ask for access request to the HIS person in GH. Knowing that the request is the need to know policy, HIS person in GH will allow access to the MOH.

DiHIS security specification language represents the need to know policy.

Ħ_MOH ∉ Λ

⊥ Ħ_MOH request +(access) $\Im_i$ ⇨ Ħ_GH

Ħ_GH ∈ Λ

⊥ Ħ_GH delegate Ħ_MOH ⇨($\Im_i$), (+access), ($\Im_{i\_size}$) ($t_{duration}$), (tɤ), ($t_{expiry}$)

Ħ _GH send $\Im_i(t) = [Þi, \Sigma j, Ħ\_GH]$ ⇨ Ħ_MOH

Ħ_GH +(update) $\Im_i$ (tɤ+Δt) = $[Þ_i, \Sigma_k, Ħ\_GH]$

⊥ Ħ_GH send μ ⇨ ∀ Ħ

The statement Ħ_GH delegate Ħ_MOH ⇨($\Im_i$), (+access), ($t_{duration}$),(tɤ),($t_{expiry}$),($\Im_{i\_size}$) represent that the information provider ( HIS person in Government Hospital) delegate to HIS person in MOH to the clinical record i, the delegate time start, and the delegate time expirers.

If the valid time of delegation has expired, then the access at Ħ_MOH will be denied.

⊥ tɤ ≤ $t_{duration}$ ≤ $t_{expiry}$

⊥ Ħ_MOH +σ

Else Ħ_MOH -σ

If ⁷Ħ_MOH need to extend the duration time, then resend the request.

### 5.2.3 Insurance companies

Insurance companies offer a number of insurance that covers different medical complexity and comes with a flexible package that is affordable by the potential customer. There are hundreds of insurance companies nowadays and they have their own policy to conduct the deal.

Let assume a situation Patient x is covered by the Insurance Y. The patient x is admitted into a hospital after he meets an accident. The hospital staff at registration counter will

ensure whether patient x have insurance or not. How to find out? Usually, the insurance company will issue an insurance card as a proof. When she found that patient x is covered by insurance, she will request the patient x's detailed insurance information; the type of insurance covered; the maximum payment allowed for the room charges, the type of ward class, and many more. This information will be send to the hospital by the insurance staff after a valid authorization has been performed. After they received the information, the hospital staff will arrange the suitable transaction for the patient x. The person in insurance company will wait for the notification of patient x's release from the hospitals. The hospitals staff will inform the insurance company's staff the bill of the hospitals at the same time.

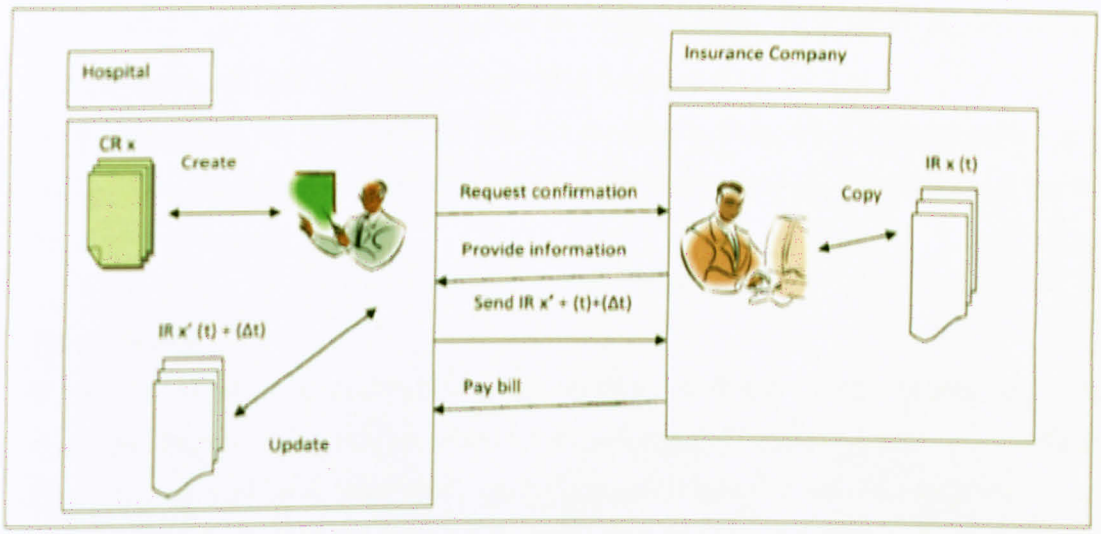


**Figure 30 Connection between hospital and insurance company**

Figure 30 above shows the connection between insurance company and hospital. When a patient x admitted to the private hospital (PH), his clinical record created by the clinician who is treating him (z). Automatically, that clinician z will be added into patient x's clinical record. The HIS person in PH will request the insurance information of patient x from the HIS person in that particular insurance company (IC).

H_PH request $\breve{I}(x) \Rightarrow$ H_IC

$\Vdash$H_IC $\in$ E

$\perp$ H_IC send $\breve{I}_x(t) \equiv [P_x, \breve{I}\_Type, \breve{I}\_Max(\$), Room\_Class, H\_IC] \Rightarrow$ H_PH

H_PH +(update) $\Im_x \wedge$ +(update) $\breve{I}(x)$

$\int P_x$ /PH

$\perp$ H_PH send $\check{I}_x(t\tau)+(\Delta t) \equiv [Þ_x$, Medic_Charge, Room_Charge, H_IC]$\Rightarrow$ H_IC

H_PH +(update) $\Im_x$ $(t\tau+\Delta t) \equiv [Þ_x, \Sigma_k$, H_KL]

$\perp$ H_PH send $\mu \Rightarrow \forall$ H

The $\check{I}(x)$ denotes insurance information belong to patient X.

$\perp$ H_IC send $\check{I}(x) \equiv [Þx$, $\check{I}$_Type, $\check{I}$_Max($), Room_Class, $\check{I}$_IC] $\Rightarrow$ H_PH denotes HIS person in IC send the copy of insurance information contained X's personal information, insurance type, maximum charges covered by insurance, room class, and the ID of the sender to the requestor ( HIS person in PH).

H_PH +(update) $\Im_x \wedge$ +(update) $\check{I}(x)$ denotes that HIS person in PH will update the clinical record of patient X and update the insurance information record of the patient X.

$\int PT_x/PH$ denote that when patient X allowed discharge from the PH.

H_PH send $\breve{I}_x(t)+(\Delta t) \equiv [Þ_x$, Medic_Charge, Room_Charge, H_IC]$\Rightarrow$ H_IC denotes that HIS person in PH send medical bill to the HIS person in IC.

At the same time, the HIS person in PH will send the updates clinical record patient X to all H units. This operation end when the insurance company pays the bills and the PH received the payment.

### 5.2.4 School

It's a must for medical assistant (MA) and nurses to come to primary school for yearly check up. They will have the schedule for all schools that located in their neighborhood. Each student will have their own medical record created at the first year they enter school. After each check performed, the record will be updated. This record must be confidential only between the MA and the guardian or parent of the student. Usually, in special cases that require the student to have a further check up, the MA will issue a letter and hand it to the student, asking them to hand in the letter to his/ her parents. The medical records for each student are confidential from any access even though by the staff of the school itself.

In the other hand, there still cases that are acceptable for the school staff such as the teacher to be acknowledge. In case of chronic disease such as heart attack or allergic to some food or medicine, is a must for the school staff to be acknowledged so that they can take reasonable precaution steps. For instance, if one student suffers a heart problem, he

must be excused from any active sport and co-curriculum activities. This can only happen when the teacher inside the school realized the disease the student is suffering.

The student's medical information will be saved until an acceptable date of expired. The set of medical assistant represented as $MA_n = \{MA_1, MA_2, MA_3, \ldots MA_x\}$ where n is a natural number that is greater than or equal to one and it's infinity. A set of student's medical record represented as $MR_k = \{MR_1, MR_2, MR_3, \ldots MR_x\}$ where x is a natural number that is greater than or equal to one and it's infinity.}

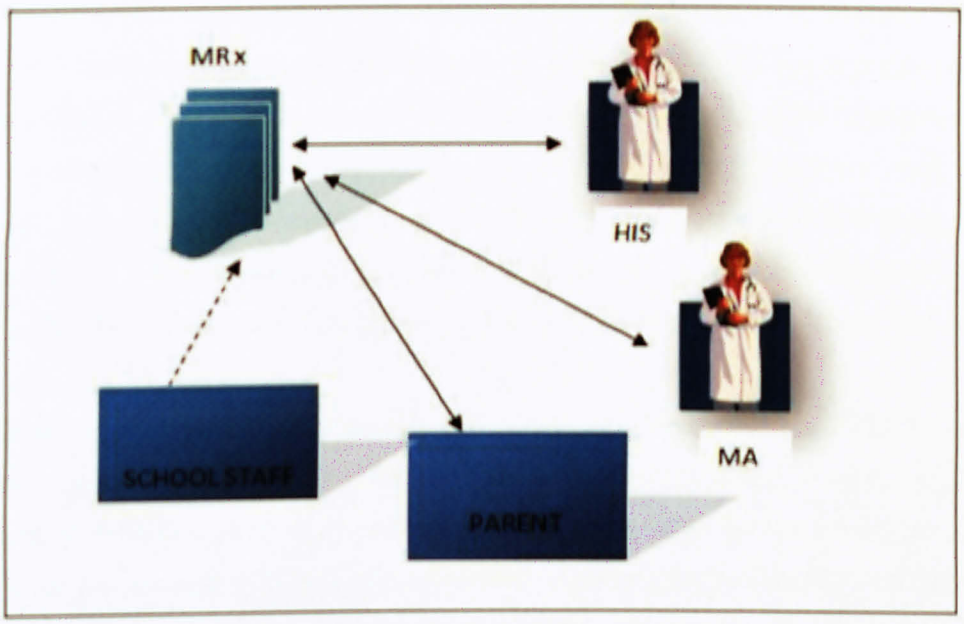


**Figure 31 Connection between clinics and schools**

Below DiHIS represent the policy.

$ACL = \{(MRx, MA_i)\}$

$\Diamond$ Emergency

$\therefore MA_i +(informParent) \wedge MA_i +(informSchoolStaff)$

$|MA_i \in ACL$

$ACL = \{(MRx, MA_i)\}$ denotes medical record student x is mapped to medical assistant i which perform the checking on the student x.

The confidentiality of the student medical record will be kept unless in case of emergency. $MA_i +(informParent) \wedge MA_i +(informSchoolStaff)$ denotes that medical

assistant i must inform parent of the student as well as the school staff for further check up and proper precaution step can be taken.

The student's medical information will be saved until an acceptable date of expired

$\oplus$ $D_{today} = D_{expiry\_date}$

$\therefore E \boxtimes [CR, \alpha]$

$| E \in ACL$

### 5.2.5 Medical Research

Research is an ongoing process. Research activities are crucial to all industry. To have research activities by our side, improvement of certain drawbacks can be achieved in the future. Health care research requires very strict policy for protecting the confidentiality of the clinical record. In medical field, the research involved the diagnoses result of one patient so that the common symptom of the disease can be determined. The main concern is to remove the actual name of the patient from the information. Common method used in hiding the patient's name is to assign a special identification code for each clinical record.

This process can be executed by the HIS person and the researchers. The researchers usually are part of the clinician themselves. They will need to submit a request to the HIS person at the units. They must provide a valid identification before the request can be accepted for processing. It will take sometimes to make a copy of the clinical record and taking out the name of the patients. After assigning special identification code, then it will be available to the requestor.

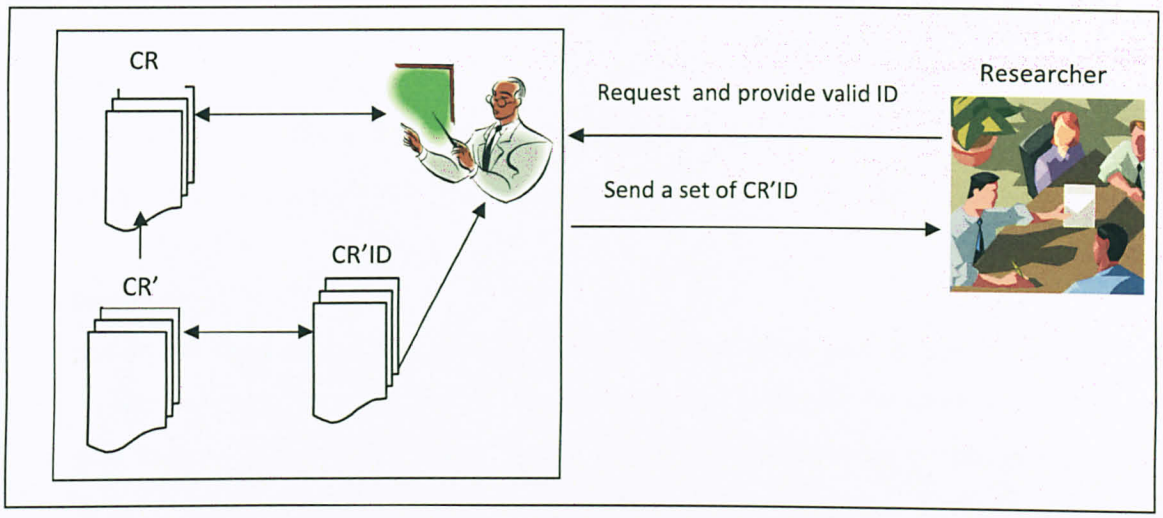


**Figure 32 Connection between hospitals and medical researchers**

This policy involving the clinical record with researcher will lead to two different operations. That would be the operation system and HIS person responsibility. The hospitals represents as Government Hospital (GH). The operation system is it must make a copy of the clinical record and then hide the real identification of these records. Then, it must assigned special code or ID as substitute of the name for each of the clinical record's owner. After this process completed, the HIS person is responsible to send this data to the (requestor) medical researcher.

These are steps performed by the system:

$\alpha$ : copy (CR $\rightarrow$ CR'')

$\alpha$: hide_name (CR'' $\rightarrow$ CR')

$\alpha$: assign ID (CR'$\rightarrow$ CR'ID)

These are steps performed by the HIS person in GH

$^{\tau}$H_Research request +(read) CR $\Rightarrow$ $^{\tau}$H_GH

$^{\tau}$H_GH send CR'ID $\Rightarrow$ $^{\tau}$H_Research

$\alpha$ : copy (CR $\rightarrow$ CR'') indicate system duplicate a set of clinical record and the value represents as CR''.

α: hide_name (CR'' → CR') indicate system hide the real name from each clinical record and the value return is CR'

α: assign ID (CR'→ CR'ID) indicate the system assigned a special code to represent the clinical record identity and the value from those operation known as CR'ID.

### 5.2.6 Employer

Employer has the right to see the medical history of their employee. It has become common when one apply for a job, besides the payment, they will look for other benefits such as easy loan for cars, loan for house, health benefit for the employee as well as the family. With these kind of offer, without knowingly, the employee and their family health is in jeopardize situation. Since their (the employee) medical history and records are available for these persons to view, they are vulnerable to discrimination. Many example situation happened and experience by employee who themselves having chronic disease being denied their insurance and in worst cases, they being lay off from the work. This is the situation that needs very careful attention to find for a solution. Employer having the permission to view their employee medical record is acceptable because they are paying for the insurance. We must restrict what information they can view to prevent discrimination towards the employee.

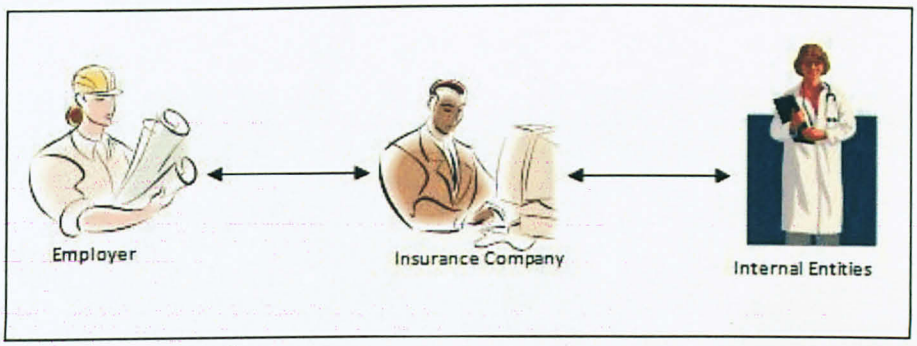


**Figure 33 Connection among Employer, Insurance Companies, hospitals, and clinics**

Figure above shows the connection among employers, insurance companies, hospitals, and clinics. This diagram represents the general connection among these organizations. Since the employer mostly associate with insurance companies for the reason that their employee covered with insurance offered by these insurance companies. Every time the

employee went to panel clinics and hospitals to get some treatment and medical, they will be needed to fill in some form stating which companies they belong and staff number for instance. In this case, we can see that the personal and clinical record is distributed into through within the system. In other words, it becomes redundant. There's a need to have suitable policy as solution of this problem. This redundancy problem is not covered in this research and left for future work.

### 5.2.7 Labs

Each hospitals and clinics have its own laboratory to perform test such as blood test. In some cases, small clinics rarely have their own laboratory. Indeed, when they need a test to performed, they will send the sample to other lab. This is a good connection, but we will need HIS in order to give chance for them to get faster result of the test performed.

In an epidemic case, there have been regulations that health district staff will assigned several labs as the testing lab. And usually these labs situated at different places and require time to transfer the result to the requestor such as health district office or state health department. There a need for system so that authorized district health office and state health department easily getting the result information in detailed. This saves time for them to make further decision for minimizing the risk and coming out with prevention and cure procedures.

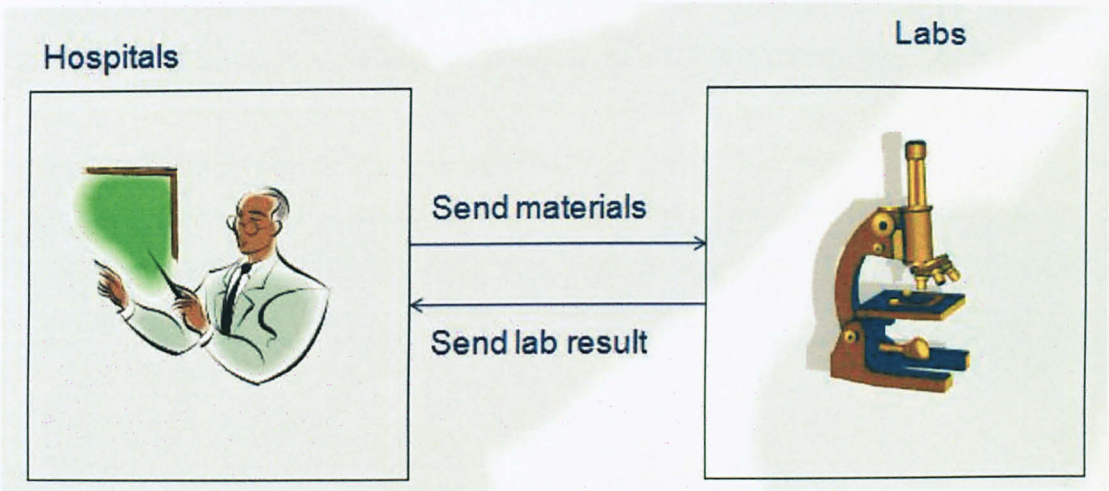


**Figure 34 Connection between hospitals and labs**

The connection between lab and hospitals or clinics is not complicated. We can see direct relationship between requestor and receiver. With the adoption of HIS, the lab result can be retrieve faster. Material is raw material such as blood, urine and etc that need to be tested in the lab. So, term material will represent as a set of $\propto_i = \{\propto_1, \propto_2, \propto_3, \ldots \propto_k\}$. The value lab result represented as a set of $\infty_t = \{\infty_1, \infty_2, \infty_3, \ldots \infty_d\}$ where i and t is a natural number that is greater than or equal to one and it's infinity.

Below DiHIS representing the policy.

$^{\tau}$H_GH send $\propto$ ⇨ $^{\tau}$H_Lab

$^{\tau}$H_ Lab send $\infty$ ⇨ $^{\tau}$H_ GH

In case a HIS person from MOH request to view the lab test result, then the policy would be represented this way: Of course the request granted after HIS person in Labs recognized that the requestor provide identity. This to prevent fraud and unauthorized access to the sensitive information.

$^{\tau}$H_ MOH request $\infty$ ⇨ $^{\tau}$H_ Lab

$^{\tau}$H_ Lab send $\infty$ ⇨ $^{\tau}$H_ MOH

### 5.2.8 Universities and Colleges

Generally, inside one education institution they have installed a clinic inside the campus. This is very useful for student who needs treatment as an outpatient such as flu, fever, gastric, headache, and sore throat. This is where the clinical records of each student saved inside the clinic panels that belong to that particular education institution. The access control lists belong to the doctor or medical assistant that entertain the student. Since the clinic inside campus is small, the number of doctor or medical assistant also small, it seems like each student clinical record belong to the same doctor. Other cases such as dental problem will be referred to other clinic. In case of chronic disease, they would refer the student to the hospital. Student is assume as patient (PT). Below the policy presented with DiHIS:

ACL = $\{(CRx, DOC_i)\}$

⌖ ChronicDisease

$\therefore DOC_n$ +(referPT ) ⇨ GH

$|DOC_n \in ACL$

$ACL = \{(CRx, DOC_i)\}$ denotes as access control list that store clinical record student x with the doctor i as the authorized person.

In case student who are taking medical course, they will be dealing with the real life cases in their course. Sometime, when we went to the hospitals, we can see practical doctor is treating a patient. Let say they are coming for internship, they access granted for them must be strictly put into a reasonable time frame. They cannot be allowed to access sensitive information without the endorsement from the responsible clinician or supervisors or HIS person. They cannot have the access unless they have the agreement from the responsible doctor or supervisor.

A set of medical student who are undergoing the internship represented as $ST_n = \{ST_1, ST_2, ST_3, \ldots ST_y\}$ where n is a natural number that is greater than or equal to one and it's infinity. Each student might be assigned at different department inside the hospital. There we have a set of department DE. We declare as $Intern = \{(ST_n, DE_i)\}$ which map student n with department i. Policy for intern student:

$|ST_n \in Intern$

$^{r}H\_$ PH delegate $ST_n \Rightarrow (CR_i), +(access), (M_{duration}), (D_{start}), (D_{expiry})$

$ST_n + (access)\ CR_y$

The policy above represent the HIS person hospital delegate to student internship to clinical record i, with a list of allowed action, the duration of the internship, as well as the start date and end date. When the expiry dates approach, the delegation will be automatically denied. Below is the representation.

$\dotplus\ D_{start} \leqslant D_{duration} \leqslant D_{expiry}$

$\therefore ST_n + \sigma$

Else $ST_n - \sigma$

### 5.2.9 Police or/and Attorney

Police or attorney's special authority ensures that they can obtain personal health information from the hospitals about some cases without any restriction regardless the

concern of privacy. However, any communication between hospitals and the authority group of people has set several procedure of action. This thesis presented three different manner of communication between these two groups diagrammatically.

In order to describe the first two ways of communications, assume a situation where an accident happened and the victim has been admitted to a hospital for proper treatment. When the victim has been admitted into the hospital, the hospital's staff gives the police a call to inform about this case. Then, the policeman comes to the hospital to meet the victim for investigation. But first, the policeman who came to the hospital will head to the receptionist and the receptionist will head him to the on duty matron. She will guide the policeman to the victim's place. Below is the diagram showing the communication flow.

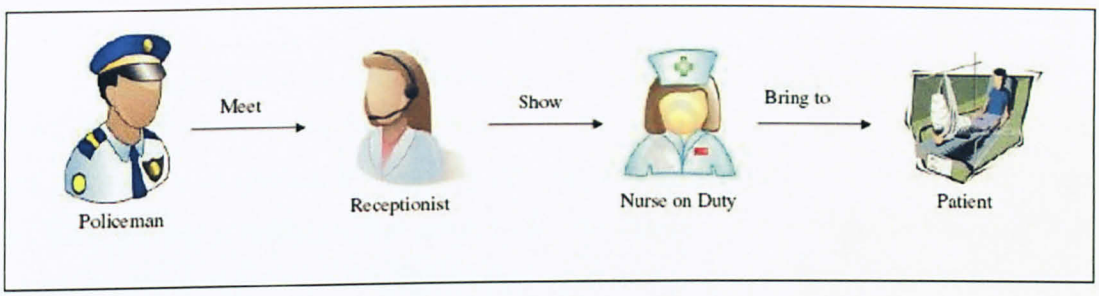


**Figure 35 The flow police to obtain information from patient**

In case the policeman wish to have knowledge about the medical or health condition of the victim, then the nurse will head the policeman to the physician who treated the victim. This personal medical information can only spoke out by the physician. Below is the diagram showing the flow.

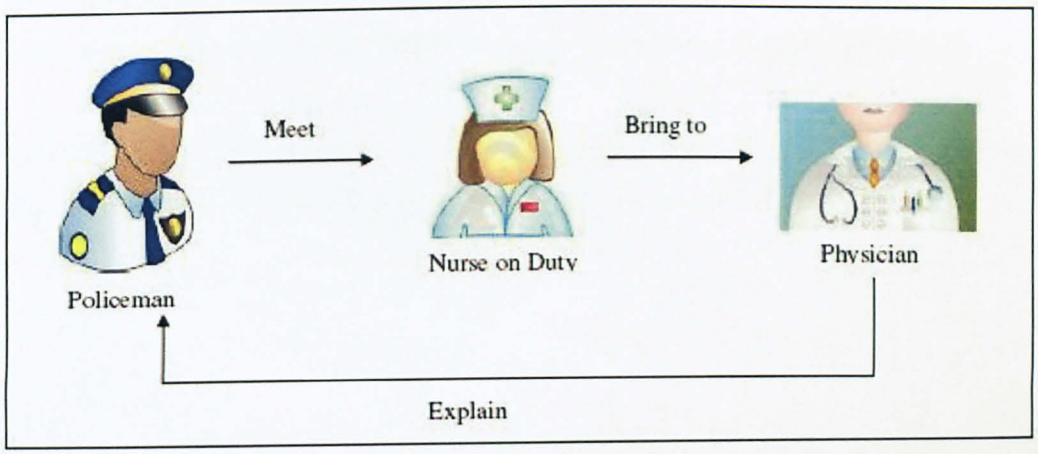


**Figure 36 Flow police to obtain health information from the physician**

The third communication to be discussed is how the police obtain the medical report in case the victim of the accident died. The policeman came to the hospital and he will be directed to the forensic pathologist who conducts the post-mortem of the body. Only an authorized physician can exposes the medical report (cause-of-death) to the authorized authority people.

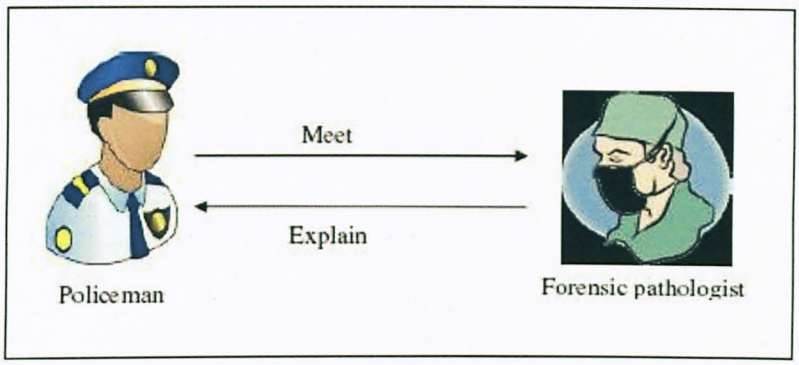


**Figure 37 Flow for police to obtain cause-of-death report from forensic pathologist**

From the case study conducted, several situations have been presented in term of sharing and transaction of clinical record. The prototype created in diagram. From the diagram, we have derived a mathematical notation for the diagram. Then, represent them in a set notation. From here, several relationships build and discusses. The policy rise from the connection also had been representing by the DiHIS security specification language. Each connection among the entity is discussed and represented by the DiHIS security specification language. The obligation and delegation policy too been applied in some sharing scenario. The case study also suggests some rules that must be adhered in order to have secured sharing information among entity within distributed HIS. Here, the need to know policy is discussed and DiHIS has been representing the policy explicitly.

This languages has not cover the information filtering policy which also an important policy within distributed HIS. This language has not solved the concept of redundancy.

# CHAPTER SIX

# CONCLUSION AND FUTURE RECOMMENDATION

In this chapter, we will be discussing the overall conclusion derived from the research conducted and the testing of the language into an application domain. The strengths as well as the limitation of the language are presented. Adding to that, suggestions for future recommendations are presented in order to improve the language as to make it better and functional in real life application.

## 6.1 Conclusion

Looking back at the three objectives initiated earlier for the completion of this research, this research manages to achieve all those objectives. The first objective stated in the first chapter said this research is going to design a security specification language for distributed Health Information System (HIS). In Chapter 4, we have presented a new security language called DiHIS-security specification language for policy based

management. We also presented the semantics rules of the language for each policy that lies under the policy based management. The symbols and their meaning which are being used throughout this language can be found in the first few pages of this thesis. We have created this language based on the Set Theory where we aimed to represent those policies mathematically.

Having the language to represent the security model for clinical information system becomes our second objective. The security model for clinical information system is a security policy model initiated in 1996 by Ross J. Anderson to overcome confusion raised during the early years of the introduction of information system. This security policy model consists of 9 principles related to clinical information system. DiHIS – security specification language has successfully able to represent all 9 principles compared to three others security languages. Those languages that are used as comparison are ASL, LaSCO and Ponder. The table of summary of the comparison clearly showed that DiHIS – security specification language is able to represent the security policy model explicitly compared to the three languages.

This research does not end there. The most challenging part is to test DiHIS – security specification language in an example of distributed HIS application domain. The application domain which consists of several organizations related to HIS has been explained and presented in Chapter 5. The organizations include the Ministry of Health, State Health Departments, District Health Offices, Public and Private Hospitals and Clinics, Police and Attorneys, Universities, Colleges, Insurance Companies, Employers and many more. The relationship occurs among them are discussed one by one. The policies of shared and exchanged information are derived from those relationships and connections. Hence, DiHIS – security specification language is used to represent those policies and it can be said DiHIS has successfully represented those policies. At this point, we come to the end of the research where we have successfully achieved all the objectives.

Completing this research does not mean that this work is complete. There are limitations that need to undergo a deep study and areas to improve DiHIS – security specification language to be implemented in real world application.

## 6.2 Future Recommendation

Technology is a kind of knowledge that is growing bit by bit. Hi-technology does not exist out of sudden. It is a process that evolved from time to time. Thus, it is impossible to claim that this work is complete and has no limitation at all. There are areas that need to be improved so as to bring this language at a higher practice and level.

In Chapter 5, there is an example of distributed HIS application domain which was used to test the ability of DiHIS – security specification language. The real life distributed HIS are dynamically changing. At one time, there could be a new organization added or removed from the system. DiHIS – security specification language should be tested in these dynamic distributed HIS environment. Having a positive result from this testing will really add the credibility of this language. It will show that DiHIS – security specification language is able to adapt to dynamically changing environments, which is the current trend of HIS. As an indirect benefit, the ability to adapt to dynamic changes can help the organization to reduce cost in the management area.

Since the application domain in Chapter 5 was an example of distributed HIS, there could be a very good opportunity if the language can be tested in real life distributed HIS environment. The term 'distributed' itself brings us to such heterogeneous system widely situated and connected to each other. In order to confirm DiHIS – security specification language ability to support distributed HIS, testing in real life distributed HIS is the most excellent way to accomplish the idea. Having this opportunity on hand, it is going to demonstrate the lack of DiHIS – security specification language and it gives a clear picture of which areas that need to be improved.

DiHIS is a security specification language for policy based management. This thesis covers seven most crucial security policies. Those policies have been explained in Chapter 4. We are aware that there are other security policies that are not covered in this thesis. The example is Filtering Information Policy. Adding more security policies into the language would add the credibility and helps the language closer to be a complete policy based management tool.

Last but not least, DiHIS security specification language should have its own tool. For instance, the Z Language has its own tool called Z-Eves software. Having its own tool,

we can assist the policy maker and executer to execute an accurate policy. In addition, it helps to detect any conflicts in the policy as well as proofing the language.

Above are several areas that are left for future work. The contribution of this work can be significantly experienced by the HIS users if all those stated recommendation can be executed successfully. Since security is a very essential issue, we will always need to find the solution as soon as possible.

## References

from http://en.wikipedia.org/wiki/Need_to_know.

(August 2007). ICT Security Policy M. o. H. Malaysia.

(May 2003). Recommended Guidelines and Standards for Practice of Telemedicine in India. D. o. I. T. (DIT), Technical Working Group on Telemedicine Standardization.

ALLAN HEYDON, M. W. M., J. D. TYGAR, JEANNETTE M. WING and AMY MOORMANN ZAREMSKI (1990). Mir6: Visual Specification of Security. IEEE Transaction on Software Engineering. **16:** 1185-1197.

Anderson, J. G. (1997). "Clearing the Way for Physicians' use of Clinical Information System." Communications of the ACM **40**(8): 83-90.

Anderson, R. J. ( Jan 1996). Security in Clinical Information Systems.

Anderson, R. J. (May 1996). A Security Policy Model for Clinical Information System. Proceeding of the IEEE Symposium on Research in Security and Privacy, Research in Security and Privacy, Oakland, CA, IEEE Computer Society Press.

Becker, M. Y. (2006). "Information Governance in NHS's NPfIT: A Case for Policy Specification." International Journal of Medical Informatics **76**(5-6): 432-437.

Bernd Blobel, P. P. (2007). "A Model Driven Approach for the German Health Telematics Architectural Framework and Security Infrastructure." International Journal of Medical Informatics(76): 169-175.

Blobel, B. (2001). "OnConet: A Secure Infrastructure to Improve Cancer Patient's Care." International Journal of Medical Informatics.

Blobel, B. (2002). "Trustworthiness in Distributed Electronic Healthcare Records- Basis for Shared Care." International Journal of Medical Informatics.

C. Abuo Zahr, T. Boerma (Aug 2005). "Health.Information System: The Foundation of Public Health." Bulletin of World Health Organization: The international Journal of Public Health **83**(8): 578-583.

Carla AbouZahr, T. B. (2005). "Health Information System: The Foundations of Public Health." International Journal of Public Health

Carlos Ribeiro, A. Z., and Paulo Ferreira (2001). SPL: An access control language for security policies with complex constraints. In Network and Distributed System Security Symposium (NDSS '01)**:** 89-107.

Chaminda, C. J. (Jul 2004). "Ethical Issues Surrounding the Use of Information in Health Care." Malaysian Journal of Library and Information Science **9**(1): 69-80.

Damianou, N. C. (February 2002). A Policy Framework for Management of Distributed Systems. Imperial College of Science, Technology and Medicine, University of London. **Doctor of Philosophy:** 233.

Guy Edjlali, A. A., and Vipin Chaudhary (1998). History-based Access Control for Mobile Code. Conference Proceedings of the 5th ACM conference on Computer and Communication Security, San Francisco, California, US, ACM.

Harel, D. (May 1988). On Visual Formalisms. Communication of the ACM. **31:** 514-530.

Hedi Hamdi, A. B. a. M. M. (October 2007). A Software Architecture for Automatic Security Policy Enforcement in Distributed System. IEEE International Conference on Emerging Security Information, System and Technologies., IEEE.

Hoagland, J., Raju Pandey, and Karl Levitt (July 1998). Security Policy Specification Using a Graphical Approach. Technical report CSE-98-3, The University of California.

J. Lavanya, K. W. G., Y. H. Leow, M. T. W. Chio, K. Prabaharan, E. Kim, Y. Kim and C. B. Soh (2006). Distributed Personal Health Information Management System for Dermatology at the Homes for Senior Citizens. Proceedings of the 28th IEEE EMBS Annual International Conference, New York City, USA.

J.Michele, J. C. (1999). The Use of a Formalised Risk Model in NHS Information System Development, University of Glasgow.

Jai Mohan, R. R. R. Y. (2004). "The Malaysian Telehealth Flagship Application: A National Approach to Health Data Protection and Utilisation and Consumer Rights." International Journal of Medical Informatics **73**: 217-227.

Jaijit Bhattacharya, S. K. G., Bhurvi Agrawal (2006). Protecting Privacy of Health Information Through Privacy Broker. Proceedings of the 39th Hawaii International Conference on System Sciences, IEEE.

Jajodia, S., Pierangela Samarati, and V.S. Subrahmanian (1997). A Logical Language for Expressing Authorizations. Proceedings of the 1997 IEEE Symposium on Security and Privacy, Oakland, CA, USA, IEEE Press.

Jajodia, S. S., P.; Subrahmanian, V.S.; (4-7 May 1997 ). A logical language for expressing authorizations. In Proceeding of the 1997 IEEE Symposium on Security and Privacy, Oakland, CA, U.S.A, IEEE Press.

Kainhofer, B. K. A. a. R. (2000). Modeling and Validating Hybrid Systems Using VDM and Mathematica.

Lampson, B. W. (1974). Protection. ACM Operating System Review, ACM.

Lamsweerde, A. v. (2000). Formal Specification:A Road Map. In the future of Software Engineering, A.Finkelstein (ed), ACM Press.

Leonidas Lymberopoulos, E. L. a. M. S. (2002). An Adaptive Policy Based Management Framework for Differentiated Services Networks. Proceeding of 3rd IEEE Workshop on Policies for Distributed Systems and Networks, Monterey, California.

Liang Xiao, A. P., Paul Lewis, Srinandan Dashmapatra, Carlos Saez, Madalina Croitoru, Javier Vicente, Horacio Gonzales-Velez, Magi Lluch i Ariet (2007). An Adaptive Security Model for Multi-agent Systems and Application to a Clinical Trials Environment. 31st Annual International Computer Software and Applications Conference (COMPSAC 2007), IEEE.

Lupu, E. C., and M. Sloman. A Role-Based Framework for Distributed Systems Management. Department of Computing. London, U. K., Imperial College. **Ph.D. Thesis**.

Lupu, E. C. a. M. S. S. (1997). "Towards a Role Based Framework for Distributed Systems Management." *Journal of Network and Systems Management* **5**(1): p. 5-30.

Muhammad Sher, T. M. (2007). 3G-WLAN Convergence: Vulnerability, Attacks Possibilities and Security Model. 2nd International Conference on Availability, Reliability and Security (ARES'07), IEEE.

Nicodemos Damianou, N. D., Emil Lupu, Morris Sloman (15 July 2002) "Ponder: A Language for Specifying Security and Management Policies for Distributed Systems." **Volume**, DOI:

Nicodemos Damianou, N. D., Emil Lupu, Morris Sloman (2001). The Ponder Policy Specification Language. Workshop on Policies for Distributed Systems and Networks. Bristol, UK: pp. 18-39.

O'Conor, R. (15 May 1999) "Commentary: Organisational and Cultural Aspect are also Important." **Volume**, DOI:

Rafae Bhatti, K. M., and Arif Ghafoor (2006). Policy-Based Security Management for Federated Healthcare Databases (or RHIOs). Proceedings of the International Workshop on Healthcare Information and Knowledge Management., Arlington, Virginia, USA, ACM.

Ramos, L. (2007). Health Network Finds Remedy in Internet Prorocol (IP). Enterprise Solution. **August/September:** 24-25.

Sandhu, R. K. T. a. R. S. (August 11-13, 1997). Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented

Authorization Management. Proceedings of the IFIP WG11.3 Workshop on Database Security,, Lake Tahoe, California.

Sandhu, R. S., E.J. Coyne, H.L. Feinstein, and C.E. Youman (1996). Role-Based Access Control Models. IEEE Computer.

Sanjeev Khanna, J. S. N., and Dan Raz (2002). Control Message Aggregation in Group Communication Protocols. 29th International Colloquium on Automota, Language and Programming (ICALP 2002), Malaga, Spain, Springer-Verlag Berlin Heidelberg.

Sheera Rosenfeld, S. K., Sharon Siler (June 2007). Privacy, Security, and the Regional Health Information Organization, California Health Care Foundation.

Sloman, E. L. a. M. (1999). Conflicts in Policy-based Distributed Systems

Management. IEEE Transactions on Software Engineering.

Sloman, M. S. (1994). "Policy Driven Management for Distributed Systems." Journal of Network and Systems Management **2**(4): p. 333-360.

Spivey, J. M. (1992). The Z Notation: A Reference Manual, Programming Research Group

University of Oxford.

Stokes, P. (2005). Privacy and Security Issues of a National Health Information Network. Department of Biomedical Engineering. Austin, University of Texas,.

Verma, D. C. (March 2002). Simplifying Network Administration Using Policy-Based Management. IEEE Network Megazine.

William W. Stead, M., Brian J. Kelly, MD, Robert M. Kolodner, MD (2004) "Achievable Steps Toward Building a National Health Information Infrastructure in the United State."

## Publication

1) Intan Najua Kamal Nasir, Azween Abdullah, Abdullah Sani Abd. Rahman. A Language to Represent Security Policy for Multi-Agent Health Information System, International Graduate Conference on Engineering and Sciences (IGCES), Universiti Teknologi Malaysia, Skudai, Johor, Malaysia. 23rd - 24th December 2008